New Difference Gröbner Bases and Bivariate Difference Dimension Polynomials

Alexander Levin

Abstract. We introduce a new type of Gröbner bases in free difference modules that are associated with a reduction respecting the effective order of module elements. We prove some properties of such Gröbner bases and present a Buchberger-type algorithm for their computation. Using the obtained results, we prove the existence and give a method of computation of a bivariate dimension polynomial of a finitely generated difference module that carries more module invariants than the classical difference dimension polynomial. We also show how the new invariants can be applied to the isomorphism problem for difference modules and to the equivalence problem for systems of algebraic difference equations.

Mathematics Subject Classification (2010). Primary: 12H10; Secondary: 13P10.

Keywords. Difference module, effective order, Gröbner basis, dimension polynomial.

1. Introduction

It is well-known that the classical Gröbner basis method can be used for the efficient computation of Hilbert polynomials of graded and filtered modules over polynomial rings. Similarly, the theory of Gröbner bases in free modules over rings of differential, difference and difference-differential operators developed in [15], [3] (differential case), [5, Chapter 4], [13], [7], [8], [9, Chapter 3], [16], [17] (difference and difference-differential cases) and in some other works provides methods of computation of dimension polynomials of differential, difference and difference-differential modules, as well as of the corresponding field extensions and systems of algebraic differential, difference and difference-differential equations. The important role of difference dimension polynomials is determined by at least four factors. First, a dimension polynomial associated with a system of algebraic difference equations expresses the strength of such a system in the sense of A. Einstein. (The significant role of this characteristic in the theory of equations of mathematical physics is described in [2]). The discussion of its difference counterpart can be found in [9, Chapter 7].) Second, a difference dimension polynomial of a finitely generated difference field extension (or of a system of algebraic difference equations that defines such an extension) carries certain invariants, that is, characteristics of the extension that do not change when we switch to another system of difference generators (with the corresponding change of the defining equations), see, for example, [6], [5, Chapter 6] and [9, Chapter 4]. In this connection, one should mention the results on multivariate difference dimension polynomials associated with partitions of the basic set of translations, see [8] and [9, Chapter 3]. It turned out that they carry more such invariants than their univariate counterparts. Third, properties of difference dimension polynomials associated with prime difference polynomial ideals provide a

This work was completed with the support of the NSF grant CCF-2139462.

powerful tool in the dimension theory of difference algebras, see [5, Chapter 7], [9, Section 4.6], and [10]. Finally, the results on difference dimension polynomials can be naturally extended to algebraic and differential algebraic structures with a finitely generated commutative group action, see [12] and [14].

In this paper we introduce the concept of a Gröbner basis in a free difference module associated with a reduction respecting the effective order of module elements. (The concept of the effective order of an element of such a module is defined as a generalization of the notion of effective order of an ordinary difference polynomial (see [1, Chapter 2, Section 4]) to the partial case.) We describe some properties of the introduced Gröbner bases and present a Buchberger-type algorithm for their computation. Then we apply the obtained results to the computation of a bivariate dimension polynomial of a finitely generated difference module M over a difference field K associated with a system of module generators. This polynomial describes the dimensions of the K-vector spaces generated by the transforms of the module generators whose orders lie between two given natural numbers. It carries more module invariants than the classical difference dimension polynomial, so we obtain a new tool for deciding whether two finitely generated difference modules are isomorphic. Furthermore, the developed technique enables us to give an alternative proof of the existence of such bivariate dimension polynomials. The first existence proof, which is based on the properties of generalized characteristic sets in a free difference module, was given in [11]. That approach, however, does not provide a method of computation of bivariate dimension polynomials, since there is no satisfactory algorithm for computing difference characteristic sets. Finally, using the properties of modules of Kähler differentials associated with field extensions, we obtain a method of computation of bivariate dimension polynomials of finitely generated difference field extensions. We conclude with examples that illustrate the advantage of applying our bivariate difference dimension polynomials to the isomorphism problem for difference modules and to the equivalence problem for systems of algebraic difference equations.

2. Preliminaries

Throughout the paper, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ denote the sets of all non-negative integers, integers, and rational numbers, respectively. If $m \in \mathbb{Z}$, $m \geq 1$, then $\leq_P$ will denote the *product order* on $\mathbb{N}^m$, that is, a partial order $\leq_P$ such that $(a_1, \ldots, a_m) \leq_P (a'_1, \ldots, a'_m)$ if and only if $a_i \leq a'_i$ for $i = 1, \ldots, m$.

By a ring we always mean an associative ring with unity. Every ring homomorphism is unitary (maps unity to unity) and every subring of a ring contains the unity. Every field is supposed to have zero characteristic. Furthermore, $\mathbb{Q}[t_1, \ldots, t_p]$ will denote the ring of polynomials in variables $t_1, \ldots, t_p$ over $\mathbb{Q}$. As usual, $\binom{t+i}{i}$ will denote the polynomial $(t+i)(t+i-1)\ldots(t+1)/i! \in \mathbb{Q}[t]$.

By a *difference ring* we mean a commutative ring R considered together with a finite set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ of injective endomorphisms of R (called *translations*) such that any two mappings α_i and α_j commute. The set σ is called the *basic set* of the difference ring R, which is also called a σ-ring. If R is a field, it is called a *difference field* or a σ-field. (We will often use prefix σ- instead of the adjective "difference".)

In what follows T denotes the free commutative semigroup generated by the set σ, that is, the semigroup of all power products $\tau = \alpha_1^{k_1} \ldots \alpha_m^{k_m}$ ($k_i \in \mathbb{N}$). The number $\operatorname{ord} \tau = \sum_{i=1}^{m} k_i$ is called the *order* of τ. Furthermore, for every $r, s \in \mathbb{N}$, $s < r$, we set

$$T(r) = \{\tau \in T \mid \operatorname{ord} \tau \leq r\} \text{ and } T(r,s) = \{\tau \in T \mid s \leq \operatorname{ord} \tau \leq r\}.$$

We consider T as an ordered set with the order $<$ defined as follows: $\tau = \alpha_1^{k_1} \ldots \alpha_m^{k_m} < \tau' = \alpha_1^{l_1} \ldots \alpha_m^{l_m}$ if and only if the $(m+1)$-tuple $(\operatorname{ord} \tau, k_1, \ldots, k_m)$ is less than $(\operatorname{ord} \tau', l_1, \ldots, l_m)$ with respect to the lexicographic order on $\mathbb{N}^{m+1}$.

A subring (respectively, ideal) S of a σ-ring R is said to be a difference (or σ-) subring of R (respectively, a difference (or σ-) ideal of R) if S is closed with respect to the action of any operator in σ. In this case the restriction of a mapping in σ to S is denoted by the same symbol. If a prime ideal P of R is closed with respect to the action of σ, it is called a *prime σ-ideal* of R. If $F \subseteq R$, then the intersection of all σ-ideals of R containing F is denoted by $[F]$. Clearly, $[F]$ is the smallest σ-ideal of R containing F; as an ideal, it is generated by the set $\{\tau(a) | \tau \in T, a \in F\}$. If the set F is finite, we say that the σ-ideal $[F]$ is finitely generated.

Let R and S be two difference rings with the same basic set σ, so that elements of σ act on each of the rings as pairwise commuting endomorphisms. (More rigorously, we assume that there exist injective mappings of σ into the sets of endomorphisms of the rings R and S such that the images of any two elements of σ commute. For convenience we will denote these images by the same symbols $\alpha_1, \ldots, \alpha_m$). A ring homomorphism $\phi : R \longrightarrow S$ is called a *difference* (or σ-) *homomorphism* if $\phi(\alpha a) = \alpha\phi(a)$ for any $\alpha \in \sigma$, $a \in R$. In this case the kernel of ϕ is a *reflexive* σ-ideal of R, that is, a σ-ideal I such that for any $\alpha \in \sigma$, the inclusion $\alpha(a) \in I$ ($a \in R$) implies $a \in I$. (Conversely, if I is a reflexive σ-ideal of a σ-ring R, then R/I has a natural structure of a σ-ring.) If I is prime then the quotient field of R/I has the natural structure of a σ-field.

If L is a σ-field and K a subfield of L which is also a σ-subring of L, then K is said to be a σ-subfield of L; L, in turn, is called a σ-field extension or a σ-overfield of K (we also say that we have a σ-field extension L/K). If $U \subseteq L$, then the intersection of all σ-subfields of L containing K and U is the unique σ-subfield of L containing K and U and contained in every σ-subfield of L containing K and U. It is denoted by $K\langle U\rangle$. If U is finite, $U = \{\eta_1, \ldots, \eta_n\}$, then L is said to be a finitely generated σ-field extension of K with the set of σ-generators $\{\eta_1, \ldots, \eta_n\}$. In this case we write $L = K\langle\eta_1, \ldots, \eta_n\rangle$. It is easy to see that $K\langle\eta_1, \ldots, \eta_n\rangle$ coincides with the field $K(\{\tau\eta_i \,|\, \tau \in T, 1 \leq i \leq n\})$. (Here and below we often write $\tau\eta$ for $\tau(\eta)$ where $\tau \in T$, $\eta \in L$.)

Let K be a σ-field and $\mathcal{U}$ a family of elements of some σ-overfield of K. We say that the family $\mathcal{U}$ is *σ-algebraically dependent* over K, if the family $T\mathcal{U} = \{\tau u \,|\, \tau \in T,\, u \in \mathcal{U}\}$ is algebraically dependent over K (that is, there exist elements $u_1, \ldots, u_k \in T\mathcal{U}$ and a nonzero polynomial f in k variables with coefficients in K such that $f(u_1, \ldots, u_k) = 0$). Otherwise, the family $\mathcal{U}$ is said to be *σ-algebraically independent* over R.

If L is a σ-overfield of a σ-field K, then a set $B \subseteq L$ is said to be a *σ-transcendence basis* of L over K if B is σ-algebraically independent over K and every element $a \in L$ is σ-algebraic over $K\langle B\rangle$ (that is, the set $\{\tau a \,|\, \tau \in T\}$ is algebraically dependent over the field $K\langle B\rangle$). If L is a finitely generated σ-field extension of K, then all σ-transcendence bases of L over K are finite and have the same number of elements (see [9, Proposition 4.1.6]). This number is called the *σ-transcendence degree* of L over K (or the σ-transcendence degree of the extension L/K); it is denoted by $\sigma\text{-tr.deg}_K L$.

Let K be a σ-field, $\sigma = \{\alpha_1, \ldots, \alpha_m\}$. With the above notation, an expression of the form $\sum_{\tau\in T} a_\tau\tau$, where $a_\tau \in K$ for any $\tau \in T$ and only finitely many elements a_τ are different from 0, is called a *difference* (or σ-) *operator* over K. Two σ-operators $\sum_{\tau\in T} a_\tau\tau$ and $\sum_{\tau\in T} b_\tau\tau$ are considered to be equal if and only if $a_\tau = b_\tau$ for any $\tau \in T$. The set of all σ-operators over K will be denoted by $\mathfrak{D}$. This set, which has a natural structure of a K-vector space with a basis T, becomes a ring if one sets $\tau a = \tau(a)\tau$ for any $a \in K$, $\tau \in T$ and extends this rule to the multiplication of any two σ-operators by distributivity. The resulting ring $\mathfrak{D}$ is called the ring of σ-operators over K. Since the set T is a basis of $\mathfrak{D}$ as a K-vector space, every nonzero σ-K-operator $g \in \mathfrak{D}$ has a unique representation in the form $g = a_1\tau_1 + \cdots + a_k\tau_k$ where $\tau_1, \ldots, \tau_k$ are distinct elements of T and $a_1, \ldots, a_k \in K$. Then the greatest and the smallest elements of the set $\{\tau_1, \ldots, \tau_k\}$ are called the *leader* and *coleader* of g, respectively. They are denoted, respectively, by u_g and v_g.

A left $\mathfrak{D}$-module is called a *difference K-module* or a *σ-K-module*. In other words, a K-vector space M is a σ-K-module, if the elements of σ act on M in such a way that $\alpha(x+y) = \alpha(x)+\alpha(y)$, $\alpha(\beta x) = \beta(\alpha x)$, and $\alpha(ax) = \alpha(a)\alpha(x)$ for any $x, y \in M$; $\alpha, \beta \in \sigma$; $a \in K$.

If M is a σ-K-module and $U \subseteq M$, then the $\mathfrak{D}$-submodule of M generated by U is denoted by $[U]$. A σ-K-module is said to be finitely generated (respectively, free) if it is finitely generated (respectively, free) as a left $\mathfrak{D}$-module. If M and N are two σ-K-modules, then a homomorphism of $\mathfrak{D}$-modules $\phi : M \to N$ is said to be a difference (or σ-) homomorphism if $\phi(\alpha x) = \alpha\phi(x)$ for any $x \in M$, $\alpha \in \sigma$.

If M is a σ-K-module, then the maximal number of elements $f_1, \dots, f_k \in M$ such that the set $\{\tau f_i \,|\, \tau \in T, 1 \leq i \leq k\}$ is linearly independent over K is called the difference (or σ-) dimension of M over K; it is denoted by $\sigma\text{-}\dim_K M$.

The following theorem proved in [6] (see also [5, Section 6.2]) introduces a Hilbert-type dimension polynomial associated with a finite system of generators of a σ-K-module.

Theorem 2.1. *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_m\}$, $\mathfrak{D}$ the ring of σ-operators over K, and M a finitely generated σ-K-module with generators $x_1, \dots, x_n$ (that is, $M = \sum_{i=1}^{n} \mathfrak{D}x_i$). For any $r \in \mathbb{N}$, let M_r denote the K-vector space generated by all elements of the form τx_i ($\tau \in T$, $1 \leq i \leq n$) with $\operatorname{ord}\tau \leq r$. Then there exists a polynomial $\phi(t) \in \mathbb{Q}[t]$ such that*

(i) *$\phi(r) = \dim_K M_r$ for all sufficiently large $r \in \mathbb{N}$ (that is, there exists $r_0 \in \mathbb{N}$ such that the last equality holds for all integers $r \geq r_0$).*

(ii) *$\deg \phi(t) \leq m$ and the polynomial $\phi(t)$ can be written as $\phi(t) = \sum_{i=0}^{m} c_i \binom{t+i}{i}$ where $c_0, c_1, \dots, c_m \in \mathbb{Z}$.*

(iii) *The integers $d = \deg \phi(t)$, c_m and c_d (if $d < m$) do not depend on the choice of the system of generators of M over $\mathfrak{D}$. Furthermore, $c_m = \sigma\text{-}\dim_K M$.*

The polynomial $\phi(t)$ is called a *σ-dimension polynomial* of the σ-K-module M associated with the system of σ-generators $x_1, \dots, x_n$.

DIMENSION POLYNOMIALS OF SUBSETS OF $\mathbb{N}^m$

A polynomial in p variables $f(t_1, \dots, t_p) \in \mathbb{Q}[t_1, \dots, t_p]$ is called *numerical* if $f(r_1, \dots, r_p) \in \mathbb{Z}$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbb{N}^p$. (It means that there exist $s_1, \dots, s_p \in \mathbb{N}$ such that the property holds for all $(r_1, \dots, r_p) \in \mathbb{N}^p$ with $r_1 \geq s_1, \dots, r_p \geq s_p$.).

Clearly, every polynomial with integer coefficients is numerical. As an example of a numerical polynomial in p variables with non-integer coefficients ($p \geq 1$) one can consider $\prod_{i=1}^{p} \binom{t_i}{m_i}$ where $m_1, \dots, m_p \in \mathbb{N}$. Note that the σ-dimension polynomial $\phi(t)$ introduced in Theorem 2.1 is a univariate numerical polynomial.

As it is proved in [5, Chapter 2], every numerical polynomial in p variables can be written as

$$f(t_1, \dots t_p) = \sum_{i_1=0}^{m_1} \dots \sum_{i_p=0}^{m_p} a_{i_1 \dots i_p} \binom{t_1 + i_1}{i_1} \dots \binom{t_p + i_p}{i_p} \tag{2.1}$$

with uniquely defined integer coefficients $a_{i_1 \dots i_p}$ (m_i is the degree of this polynomial with respect to t_i, $1 \leq i \leq p$).

In what follows, if $A \subseteq \mathbb{N}^m$ (m is a positive integer), then V_A will denote the set of all m-tuples $v = (v_1, \dots, v_m) \in \mathbb{N}^m$ such that $a \not\leq_P v$ for every $a \in A$ (i. e., for any $a = (a_1, \dots, a_m) \in A$, there exists $i, 1 \leq i \leq m$, such that $a_i > v_i$). Furthermore, for any $r \in \mathbb{N}$, we set $A(r) = \{(a_1, \dots, a_m) \in A \,|\, \sum_{i=1}^{m} a_i \leq r\}$.

The following theorem about a univariate numerical polynomial associated with a subset of $\mathbb{N}^m$ is due to E. Kolchin, see [4, Chapter 0, Lemma 16].

Theorem 2.2. *Let $A \subseteq \mathbb{N}^m$. Then there exists a numerical polynomial $\omega_A(t)$ such that*

(i) $\omega_A(r) = \operatorname{Card} V_A(r)$ *for all sufficiently large* $r \in \mathbb{N}$.

(ii) $\deg \omega_A \leq m$.

(iii) $\deg \omega_A = m$ *if and only if* $A = \emptyset$. *In this case,* $\omega_A(t) = \binom{t+m}{m}$.

(iv) $\omega_A = 0$ *if and only if* $(0, \ldots, 0) \in A$.

The polynomial $\omega_A(t)$ is called the *Kolchin polynomial* of the set $A \subseteq \mathbb{N}^m$.

Remark 2.3. As it is shown in [4, Ch. 0, Lemma 15], every infinite sequence of elements of a set $\mathbb{N}^m \times \{1, \ldots, q\}$ $(m, q \geq 1)$ has an infinite subsequence strictly increasing with respect to the product order, in which every element has the same last coordinate. (Therefore, if $A \subseteq \mathbb{N}^m$ and A' is the set of all minimal elements of A with respect to the product order, then the set A' is finite.)

The following proposition about decreasing sequences of certain subsets of $\mathbb{Z}^m$ with respect to the lexicographic order will be used in the proof of the termination of a Buchberger-type algorithm considered in section 3.

Proposition 2.4. *Let $A = \{(\sum_{i=1}^m (a_i - b_i), a_1 - b_1, \ldots, a_m - b_m) \in \mathbb{Z}^{m+1} \mid a_i, b_i \in \mathbb{N}$ $(1 \leq i \leq m), \sum_{i=1}^m (a_i - b_i) \geq 0$, and $(b_1, \ldots, b_m) \leq_{lex} (a_1, \ldots, a_m)\}$. Then A does not contain strictly decreasing sequences with respect to the lexicographic order.*

Proof. Suppose that the set A contains an infinite sequence

$$\mathbf{a_1}, \mathbf{a_2}, \ldots \tag{2.2}$$

such that $\mathbf{a_1} \geq_{lex} \mathbf{a_2} \geq_{lex} \ldots$. Let $\mathbf{a_k} = \{(\sum_{i=1}^m (a_{ki} - b_{ki}), a_{k1} - b_{k1}, \ldots, a_{km} - b_{km})$ for some $a_{k1}, \ldots, a_{km}, b_{k1}, \ldots, b_{km} \in \mathbb{N}$ with $\sum_{i=1}^m (a_{ki} - b_{ki}) \geq 0$ and $(b_{k1}, \ldots, b_{km}) \leq_{lex} (a_{k1}, \ldots, a_{km})$ $(k = 1, 2, \ldots)$. Then $\sum_{i=1}^m (a_{1i} - b_{1i}) \geq_{lex} \sum_{i=1}^m (a_{2i} - b_{2i}) \geq_{lex} \ldots$ is a decreasing sequence in $\mathbb{N}$, hence there exists $p \in \mathbb{N}$ such that $\sum_{i=1}^m (a_{pi} - b_{pi}) = \sum_{i=1}^m (a_{p+1,i} - b_{p+1,i}) = \ldots$. Therefore, without loss of generality we can assume that $\sum_{i=1}^m (a_{1i} - b_{1i}) = \sum_{i=1}^m (a_{2i} - b_{2i}) = \ldots$ in sequence (2.2). Now, since $\mathbf{a_1} \geq_{lex} \mathbf{a_2} \geq_{lex} \ldots$ and $(a_{k1}, \ldots, a_{km}) \geq_{lex} (b_{k1}, \ldots, b_{km})$ for $k = 1, 2, \ldots$, we have a decreasing sequence $a_{11} - b_{11} \geq a_{21} - b_{21} \geq \ldots$ in $\mathbb{N}$ that stabilizes, that is, there exists a positive integer q such that $a_{q1} - b_{q1} = a_{q+1,1} - b_{q+1,1} = \ldots$. Thus, without loss of generality we can assume that $\sum_{i=1}^m (a_{1i} - b_{1i}) = \sum_{i=1}^m (a_{2i} - b_{2i}) = \ldots$ and $a_{11} - b_{11} = a_{21} - b_{21} = \ldots$ in (2.2). Repeating the same argument for the third, fourth, etc., coordinates of element of the sequence (2.2), we obtain that the sequence (2.2) stabilizes at some place. This completes the proof. □

The following theorem proved in [5, Chapter 2] gives an explicit formula for the Kolchin polynomial of a finite subset of $\mathbb{N}^m$.

Theorem 2.5. *Let $A = \{a_1, \ldots, a_n\}$ be a finite subset of $\mathbb{N}^m$ and let $a_k = (a_{k1}, \ldots, a_{km})$ $(1 \leq k \leq n)$. For any $l \in \mathbb{N}$, $0 \leq l \leq n$, let $\Gamma(l, n)$ denote the set of all l-element subsets of the set $\mathbb{N}_n = \{1, \ldots, n\}$. Let $\bar{a}_{\emptyset j} = 0$ and for any $\gamma \in \Gamma(l, n)$, $\gamma \neq \emptyset$, let $\bar{a}_{\gamma j} = \max\{a_{ij} \mid i \in \gamma\}$ $(1 \leq j \leq m)$. Then*

$$\omega_A(t) = \sum_{l=0}^{n} (-1)^l \sum_{\gamma \in \Gamma(l,n)} \binom{t + m - \sum_{j=1}^m \bar{a}_{\gamma j}}{m} \tag{2.3}$$

3. Gröbner bases respecting the effective order

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_m\}$ and F a free σ-K-module with free generators $f_1, \dots, f_n$ (i. e., these elements form a basis of the free left module F over the ring of σ-operators $\mathfrak{D}$ over K). In what follows, elements of the form τf_ν ($\tau \in T, 1 \leq \nu \leq n$) will be called *terms*; the set of all terms will be denoted by Tf. Clearly, Tf is a basis of F treated as a K-vector space.

The order of a term $u = \tau f_i$ (denoted by $\operatorname{ord} u$) is defined as the order of τ. If $\tau, \tau' \in T$, we say that τ divides τ' (and write $\tau \mid \tau'$) if $\tau' = \tau\tau''$ for some $\tau'' \in T$. In this case we write $\tau'' = \frac{\tau'}{\tau}$. If $u = \tau f_i, v = \tau' f_j \in Tf$, we say that u divides v (and write $u|v$) if $i = j$ and $\tau|\tau'$. We also say that v is a *transform* of u and define the ratio $\frac{v}{u}$ as $\frac{\tau'}{\tau}$. The least common multiple of two terms $u = \tau_1 f_i$ and $v = \tau_2 f_j$ is defined as usual: $\operatorname{lcm}(u, v) = \operatorname{lcm}(\tau_1, \tau_2) f_i$ if $i = j$ and $\operatorname{lcm}(u, v) = 0$ if $i \neq j$.

By a *ranking* on Tf we mean a well-ordering $\leq$ of the set of terms Tf that satisfies the following two conditions:

(i) $u \leq \tau u$ for any $u \in Tf, \tau \in T$. (We denote the ordering of Tf by the usual symbol $\leq$ and write $u < v$ or $v > u$ if $u \leq v$ and $u \neq v$.)

(ii) If $u, v \in Tf$ and $u \leq v$, then $\tau u \leq \tau v$ for any $\tau \in T$.

A ranking is said to be *orderly* if the inequality $\operatorname{ord} u < \operatorname{ord} v$ ($u, v \in Tf$) implies $u < v$. In what follows, we assume that the following orderly ranking $\leq$ on Tf is fixed: if $u_1 = \alpha_1^{k_1} \dots \alpha_m^{k_m} f_i, u_2 = \alpha_1^{l_1} \dots \alpha_m^{l_m} f_j \in Tf$, then $u_1 \leq u_2$ if and only if

$$(\operatorname{ord} u_1, k_1, \dots, k_m, i) \leq_{lex} (\operatorname{ord} u_2, l_1, \dots, l_m, j)$$

($\leq_{lex}$ denotes the lexicographic order on $\mathbb{N}^{m+2}$).

Since the set Tf is a basis of the vector K-space F, every nonzero element $f \in F$ has a unique (up to the order of the terms in the sum) representation in the form

$$g = a_1\tau_1 f_{i_1} + \dots + a_p\tau_p f_{i_p} \tag{3.1}$$

where $\tau_1 f_{i_1}, \dots, \tau_p f_{i_p}$ are distinct elements of Tf ($1 \leq i_1, \dots, i_p \leq n$) and $a_1, \dots, a_p$ are nonzero elements of K.

Definition 3.1. Let g be an element of the free σ-K-module F written in the form (3.1) and let $\tau_r f_{i_r}$ and $\tau_s f_{i_s}$ ($1 \leq r, s \leq p$) be the greatest and the smallest terms in the set $\{\tau_1 f_{i_1}, \dots, \tau_p f_{i_p}\}$, respectively, relative to the introduced order on Tf. Then the terms $\tau_r f_{i_r}$ and $\tau_s f_{i_s}$ are called, respectively, the **leader** and **coleader** of the element g; they are denoted by u_g and v_g, respectively. The coefficients of u_g and v_g in g will be denoted by $\operatorname{lc}(g)$ and $\operatorname{mc}(g)$, respectively.

Definition 3.2. If $0 \neq g \in F$, then the nonnegative integer $\operatorname{ord} u_g - \operatorname{ord} v_g$ is called the **effective order** of g ; it is denoted by $\operatorname{Eord}(g)$.

It follows from the last definition that for any $g \in F$ and for any $\tau \in T$, $\operatorname{Eord}(\tau g) = \operatorname{Eord}(g)$.

Definition 3.3. Let $g, h \in F$. We say that g is E-reduced with respect to h if g does not contain any τu_h ($\tau \in T$) such that $\tau v_h \geq v_g$. If g does not contain any τv_h ($\tau \in T$) such that $\tau u_h l \leq u_g$, we say that g is E^*-reduced with respect to h. If $U \subseteq F$, then an element $g \in F$ is said to be E-reduced (respectively, E^*-reduced) with respect to U if g is E-reduced (respectively, E^*-reduced) with respect to every element of U.

Remark 3.4. It follows from Proposition 2.4 that F cannot contain an infinite sequence $h_1, h_2, \dots$ such that h_i is E-reduced with respect to $\{h_1, \dots, h_{i-1}\}$ for $i = 2, 3, \dots$. Indeed, by Remark 2.3, if such a sequence exists, then it contains a subsequence $\{h_{i_k}\}$ such that $u_{h_{i_k}} \mid u_{h_{i_{k+1}}}$, $h_{i_{k+1}}$ is E-reduced with respect to all h_{i_l} with $l < k + 1$ ($k = 1, 2, \dots$), and all elements $v_{h_{i_k}}$ ($k =$

$1, 2, \dots$) contain the same free generator f_p ($1 \leq p \leq n$). Without loss of generality we can assume that $u_{h_i} \,|\, u_{h_{i+1}}$ ($i = 1, 2, \dots$), $\left(\frac{u_{h_j}}{u_{h_i}}\right) v_{h_i} < v_{h_j}$ whenever $i < j$, and all elements v_{h_i} ($i = 1, 2, \dots$) contain the same free generator f_p. If $u_{h_i} = \alpha_1^{a_{i1}} \dots \alpha_m^{a_{im}}$, $v_{h_i} = \alpha_1^{b_{i1}} \dots \alpha_m^{b_{im}}$, $u_{h_j} = \alpha_1^{a_{j1}} \dots \alpha_m^{a_{jm}}$, and $v_{h_j} = \alpha_1^{b_{j1}} \dots \alpha_m^{b_{jm}}$, then the inequality $\left(\frac{u_{h_j}}{u_{h_i}}\right) v_{h_i} < v_{h_j}$ is equivalent to the inequality $\mathbf{a_i} >_{lex} \mathbf{a_j}$ in Proposition 2.4. However, this proposition states that there is no infinite sequence satisfying such inequalities.

Definition 3.5. Let N be a $\mathfrak{D}$-submodule of F. A finite set $G = \{g_1, \dots, g_r\} \subseteq N$ is called an E-Gröbner basis of N if for any $h \in N$, there exists $g_i \in G$ such that $u_{g_i} \,|\, u_h$ and $\frac{u_h}{u_{g_i}} v_{g_i} \geq v_h$.

A set $G = \{g_1, \dots, g_r\} \subseteq F$ is said to be an *E-Gröbner basis* if G is an E-Gröbner basis of $N = \sum_{i=1}^{r} \mathfrak{D} g_i$.

Remark 3.6. If one removes the condition $\frac{u_h}{u_{g_i}} v_{g_i} \geq v_h$ in the last definition, we obtain the definition of a "standard" Gröbner basis in a free difference module in the sense of Theorem 4.1.33 of [5] (algorithms for computing such Gröbner bases are presented in [5, Section 4.2]). The theorem gives 17 equivalent definitions of such a Gröbner basis. In particular, the fact that $G = \{g_1, \dots, g_r\}$ is a Gröbner basis of a $\mathfrak{D}$-submodule N of F is equivalent to the condition that $f \in N$ if and only if $f = \sum_{i=1}^{r} h_i g_i$ where $h_1, \dots, h_r \in \mathfrak{D}$ and $u_f = \max\{u_{h_i g_i} \,|\, 1 \leq i \leq r\}$. It follows that every E-Gröbner basis of N is also a "standard" Gröbner basis of N. Therefore, every E-Gröbner basis of N generates N as a left $\mathfrak{D}$-module.

Definition 3.7. Given $f, g, h \in F$, with $g \neq 0$, we say that the element f E-reduces to h modulo g in one step and write $f \xrightarrow[E]{\mathrm{g}} h$ if and only if f contains some term w with a coefficient a such that $u_g | w$, $h = f - a(\tau(\mathrm{lc}(g)))^{-1} \tau g$, where $\tau = \frac{w}{u_g}$, and $\tau v_g \geq v_f$.

We say that f E^*-reduces to h modulo g in one step and write $f \xrightarrow[E^*]{\mathrm{g}} h$ if and only if f contains some term w with a coefficient a such that $v_g | w$, $h = f - a(\tau(\mathrm{mc}(g)))^{-1} \tau g$, where $\tau = \frac{w}{v_g}$, and $\tau u_g \leq u_f$.

Note that both E- and E^*- reductions of an element $f \in F$ do not increase the effective order of f.

Definition 3.8. Let $f, h \in F$ and let $G = \{g_1, \dots, g_r\}$ be a finite set of non-zero elements of F. We say that f E-reduces (respectively, E^*-reduces) to h modulo G and write $f \xrightarrow[E]{G} h$ (respectively, $f \xrightarrow[E^*]{G} h$) if and only if there exists a sequence of elements $g^{(1)}, g^{(2)}, \dots g^{(q)} \in G$ and a sequence of elements $h_1, \dots, h_{q-1} \in F$ such that
$f \xrightarrow[E]{g^{(1)}} h_1 \xrightarrow[E]{g^{(2)}} \dots \xrightarrow[E]{g^{(q-1)}} h_{q-1} \xrightarrow[E]{g^{(q)}} h$ (respectively, $f \xrightarrow[E^*]{g^{(1)}} h_1 \xrightarrow[E^*]{g^{(2)}} \dots \xrightarrow[E^*]{g^{(q-1)}} h_{q-1} \xrightarrow[E^*]{g^{(q)}} h$).

Proposition 3.9. *With the above notation, let $S = \{g_1, \dots, g_k\} \subseteq F$ and $h \in F$. Then there exists an element $h^* \in F$ such that h^* is E-reduced with respect to S and $h - h^* \in [S]$.*

Proof. If h is E-reduced with respect to S, the statement is obvious (one can set $h^* = h$). Suppose that h is not E-reduced with respect to S. In what follows, if element $t \in F$ is not E-reduced with respect to S, then a term w_t that appears in t will be called the S-leader of t if w_t is the greatest term among all terms τu_{g_j} ($\tau \in T$, $1 \leq j \leq k$) that appear in t and satisfy the condition $\tau v_{g_j}) \geq v_t$.

Let w_h be the S-leader of h and let c_h be the coefficient of w_h in h. Then $w_h = \tau u_{g_j}$ for some $\tau \in T$ and for some j ($1 \leq j \leq k$) such that $\tau v_{g_j} \geq v_h$. Let us choose such j that corresponds to the maximum leader u_{g_j} in the set of all leaders of elements of S and consider the element $h' = h - \frac{c_h}{\tau(\mathrm{lc}(g_j))} \tau g_j$. Obviously, h' does not contain w_h and $u_{h'} \leq u_h$. Furthermore, h' cannot

contain any term $\tau' u_{g_i}$ ($\tau' \in T, 1 \leq i \leq k$) that is greater than w_h and satisfies the condition $\tau' v_{g_i} \geq v_{h'}$. Indeed, since $v_{h'} \geq v_h$, such a term $\tau' u_{g_i}$ cannot appear in h. Such a term cannot appear in τg_j either, since $u_{\tau g_j} = \tau u_{g_j} = w_h < \tau' u_{g_i}$. Thus, the S-leader of h' is strictly less than the S-leader of h. Applying the same procedure to the element h' and continuing in the same way, we obtain an element $h^* \in F$ such that $h - h^* \in [S]$ and h^* is E-reduced with respect to S. □

The process of E-reduction described in the proof of Proposition 3.9 can be realized by the following algorithm that clearly terminates and results in an element which is E-reduced with respect to S. (The set of terms is well-ordered and each step of the algorithm decreases the S-leader.) Also, it is easy to see that analogs of Proposition 3.9 and Algorithm I hold for the E^*-reduction.

Algorithm I. $(h, k, g_1, \ldots, g_k;\ h^*)$
Input: $h \in F$, *a positive integer* k, $S = \{g_1, \ldots, g_k\} \subseteq F$ *where* $g_i \neq 0$ *for* $i = 1, \ldots, k$
Output: $h^* \in F$ *and* $A_1, \ldots, A_k \in \mathfrak{D}$ *such that* $h = A_1 g_1 + \cdots + A_k g_k + h^*$ *and* h^* *is* E*-reduced with respect to* S
Begin
$A_1 := 0, \ldots, A_k := 0, h^* := h$
While *there exist* i, $1 \leq i \leq k$, *and a term* w, *that appears in* h^* *with a (nonzero) coefficient* c_w, *such that* $u_{g_i} | w$ *and* $\frac{w}{u_{g_i}} v_{g_i} \geq v_{h^*}$ **do**
z:= *the greatest of the terms* w *that satisfy the above conditions.*
j:= *the smallest number* i *for which* u_{g_i} *is the greatest leader of an element of* S *such that* $u_{g_i} | z$ *and* $\frac{z}{u_{g_i}} v_{g_i} \geq v_{h^*}$
$\tau := \frac{z}{u_{g_j}}$
$A_j := A_j + \frac{c_z}{\tau(\mathrm{lc}(g_j))}\tau$ where c_z *is the coefficient of* z in h^*
$h^* := h^* - \frac{c_z}{\tau(\mathrm{lc}(g_j))}\tau g_j$
End

Theorem 3.10. *Let* K *be a* σ*-field,* F *a free* σ*-*K*-module with free generators* $f_1, \ldots, f_n$, N *a* σ*-*K*-submodule of* F, *and* $G = \{g_1, \ldots, g_r\} \subseteq N$ ($r \geq 1$). *Then the following statements are equivalent.*

(i) G *is an* E*-Gröbner basis of* N.

(ii) *Let* $f \in F$. *Then* $f \in N$ *if and only if* $f \xrightarrow[E]{G} 0$.

(iii) *Every element* $f \in N$ *can be represented as* $f = \sum_{i=1}^{r} h_i g_i$ *where* $h_1, \ldots, h_r \in \mathfrak{D}$, $u_f = \max\{u_{h_i g_i} \mid 1 \leq i \leq r\}$, *and* $v_f = \min\{v_{h_i} v_{g_i} \mid 1 \leq i \leq r\}$.

Proof. (i)⇒ (ii). Clearly, if $f \in F$ and $f \xrightarrow[E]{G} 0$, then $f \in N$. Conversely, let $f \in N$. By Proposition 3.8, there exists $h^* \in F$ such that $f \xrightarrow[E]{G} h^*$, $f - h^* \in [G] = N$, and h^* is E-reduced with respect to G. If $h^* \neq 0$, then $h^* \in N$ and there exists $g_i \in G$ such that $u_{g_i} \mid u_h$ and $\frac{u_h}{u_{g_i}} v_{g_i} \geq v_h$. It contradicts the fact that h^* is E-reduced with respect to G.

(ii)⇒ (iii). Let $f \in N$. By (ii), $f \xrightarrow[E]{G} 0$. Now, the process of reduction described in the proof of Proposition 3.9 shows that $f = \sum_{i=1}^{r} h_i g_i$ for some $h_i \in \mathfrak{D}$ ($1 \leq i \leq r$) such that $u_f = \max\{u_{h_i g_i} \mid 1 \leq i \leq r\}$ and $v_f \leq \min\{v_{h_i} v_{g_i} \mid 1 \leq i \leq r\}$. Clearly, the last inequality cannot be strict, so we have the equality.

(iii)⇒ (i). If $f = \sum_{i=1}^{r} h_i g_i$ ($h_1, \ldots, h_r \in \mathfrak{D}$) and $u_f = \max\{u_{h_i g_i} \mid 1 \leq i \leq r\}$, then there exists $j \in \{1, \ldots, r\}$ such that $u_{g_j} \mid u_f$ and $u_f = u_{h_j} u_{g_j} = u_{h_j g_j}$. Since $v_f \leq \min\{v_{h_i g_i} \mid 1 \leq i \leq r\}$, we have $v_f \leq v_{h_j} v_{g_j} \leq u_{h_j} v_{g_j}$, so G is an E-Gröbner basis of N. □

Remark 3.11. The equivalence of parts (ii) and (iii) of the last theorem implies that if $0 \neq f \in F$, G is a finite subset of F, and $f \xrightarrow[E^*]{G} 0$ (hence f has a representation given in part (iii), as one can easily obtain by mimicking the proof (iii)$\Rightarrow$ (i) above), then $f \xrightarrow[E]{G} 0$. Therefore, if $0 \neq f \in F$ is already E^*-reduced with respect to G and $f \xrightarrow[E]{G} f'$, then $f' \neq 0$.

Definition 3.12. Let f and g be two elements in the free $\mathfrak{D}$-module F. Then the element

$$S_v(f,g) = \left(\frac{\operatorname{lcm}(v_f, v_g)}{v_f}(\operatorname{mc}(f))\right)^{-1} \frac{\operatorname{lcm}(v_f, v_g)}{v_f} f - \left(\frac{\operatorname{lcm}(v_f, v_g)}{v_g}(\operatorname{mc}(g))\right)^{-1} \frac{\operatorname{lcm}(v_f, v_g)}{v_g} g$$

is called the S_v**-polynomial** of f and g.

Proposition 3.13. *With the above notation, let $f, g_1, \ldots, g_r \in F$ ($r \geq 1$) and let $f = \sum_{i=1}^{r} c_i \omega_i g_i$ where $\omega_i \in T$, $c_i \in K$ ($1 \leq i \leq r$). Let $u_i = u_{g_i}$, $v_i = v_{g_i}$, and $v_{\nu j} = \operatorname{lcm}(v_\nu, v_j)$ ($1 \leq i, \nu, j \leq r$). Suppose that $\omega_1 v_1 = \cdots = \omega_r v_r = v$, $v_f > v$, and $\omega_i u_i \leq u_f$ for $i = 1, \ldots, r$. Then there exist elements $c_{\nu j} \in K$ ($1 \leq \nu \leq s$, $1 \leq j \leq t$ for some $s, t \in \mathbb{N}$) such that*

$$f = \sum_{\nu=1}^{s} \sum_{j=1}^{t} c_{\nu j} \theta_{\nu j} S_v(g_\nu, g_j)$$

where $\theta_{\nu j} = \frac{v}{v_{\nu j}}$ and $\theta_{\nu j} v_{S_v(g_\nu, g_j)} > v$, $\theta_{\nu j} u_{S_v(g_\nu, g_j)} \leq u_f$ ($1 \leq \nu \leq s$, $1 \leq j \leq t$).

Proof. Let $d_i = \operatorname{mc}(\omega_i g_i) = \omega_i(\operatorname{mc}(g_i))$ $(1 \leq i \leq r)$. Since $\omega_1 v_1 = \cdots = \omega_r v_r = v$ and $v_f > v$, $\sum_{i=1}^{r} c_i d_i = 0$. Let $h_i = d_i^{-1} \omega_i g_i$ so $\operatorname{mc}(h_i) = 1$ $(1 \leq i \leq r)$ and $f = \sum_{i=1}^{r} c_i \omega_i g_i = c_1 d_1 (h_1 - h_2) + (c_1 d_1 + c_2 d_2)(h_2 - h_3) + \cdots + (c_1 d_1 + \cdots + c_{r-1} d_{r-1})(h_{r-1} - h_r)$. (To represent an identity, the last sum should end $(c_1 d_1 + \cdots + c_r d_r) h_r$, but this term is equal to zero.)

Let $\tau_{\nu j} = \frac{v_{\nu j}}{v_\nu}$ and $\gamma_{\nu j} = \frac{v_{\nu j}}{v_j}$ $(1 \leq \nu, j \leq r, \nu \neq j)$. Then

$\theta_{\nu j} S_v(g_\nu, g_j) = \theta_{\nu j}[(\tau_{\nu j}(\operatorname{mc}(g_\nu)))^{-1} \tau_{\nu j} g_\nu - (\gamma_{\nu j}(\operatorname{mc}(g_j)))^{-1} \gamma_{\nu j} g_j] = [\theta_{\nu j}(\tau_{\nu j}(\operatorname{mc}(g_\nu)))]^{-1} \frac{v}{v_\nu} g_\nu$
$- [\theta_{\nu j}(\gamma_{\nu j}(\operatorname{mc}(g_j)))]^{-1} \frac{v}{v_j} g_j = [\omega_\nu(\operatorname{mc}(g_\nu))]^{-1} \omega_\nu g_\nu - [\omega_j(\operatorname{mc}(g_j))]^{-1} \omega_j g_j = h_\nu - h_j$. Therefore,

$f = c_1 d_1 \theta_{12} S_v(g_1, g_2) + (c_1 d_1 + c_2 d_2) \theta_{23} S_v(g_2, g_3) + \cdots + (c_1 d_1 + \cdots + c_{r-1} d_{r-1}) \theta_{r-1,r} S_v(g_{r-1}, g_r)$.

Also, $\theta_{i,i+1} u_{S_v(g_i, g_{i+1})} = u_{\theta_{i,i+1} S_v(g_i, g_{i+1})} = u_{h_i - h_{i+1}} \leq u_f$ and $v_{h_i - h_{i+1}} > v$, since the coleaders of h_i and h_{i+1} are equal and $\operatorname{mc}(h_i) = \operatorname{mc}(h_{i+1}) = 1$ $(1 \leq i \leq r-1)$. □

Theorem 3.14. *Let $G = \{g_1, \ldots, g_r\}$ be a "standard" Gröbner basis of an $\mathfrak{D}$-submodule N of F (see Remark 3.5). Suppose that $S_v(g_i, g_j) \xrightarrow[E^*]{G} 0$ for any $i, j \in \{1, \ldots, r\}$, $i \neq j$. Then G is an E-Gröbner basis of N.*

Proof. By Theorem 3.10, it is sufficient to show that every element $f \in N$ can be represented as

$$f = \sum_{i=1}^{r} h_i g_i \tag{3.2}$$

where $h_1, \ldots, h_r \in \mathfrak{D}$ and

$$u_f = \max\{u_{h_i g_i} \mid 1 \leq i \leq r\},\ v_f \leq \min\{v_{h_i} v_{g_i} \mid 1 \leq i \leq r\}. \tag{3.3}$$

Since G is a "standard" Gröbner basis of N, an element $f \in N$ can be written as

$$f = \sum_{i=1}^{r} H_i g_i \tag{3.4}$$

where $H_1, \dots, H_r \in \mathfrak{D}$ and

$$u_f = \max\{u_{H_i g_i} \,|\, 1 \le i \le r\} = \max\{u_{H_i} u_{g_i} \,|\, 1 \le i \le r\}. \tag{3.5}$$

Let us choose such a representation of f with the greatest possible term $v = \min\{v_{H_i} v_{g_i} \,|\, 1 \le i \le r\}$. (Clearly, $v \le v_f$.) Let $d_i = \mathrm{mc}(H_i)$ $(i = 1, \dots, r)$. Then the element f can be written as

$$f = \sum_{v_{H_i} v_{g_i} = v} d_i v_{H_i} g_i + \sum_{v_{H_i} v_{g_i} = v} (H_i - d_i v_{H_i}) g_i + \sum_{v_{H_i} v_{g_i} > v} H_i g_i. \tag{3.6}$$

Note that if $v = v_f$, then the representation (3.6) satisfies conditions (3.2) and (3.3). Suppose that $v_f > v$. Since $v = \min\{v_{H_i} v_{g_i} \,|\, 1 \le i \le r\}$, $v_{H_i - d_i v_{H_i}} > v$ in the second sum of (3.6). Also, it is clear that $v_{H_i} v_{g_i} = v_{H_i g_i} = v$ for any term in the sum

$$\tilde{f} = \sum_{v_{H_i} v_{g_i} = v} d_i v_{H_i} g_i \tag{3.7}$$

and $u_{\tilde{f}} \le \max\{v_{H_i} u_{g_i} \,|\, i \in I\} \le \max\{u_{H_i} u_{g_i} \,|\, i \in I\} \le u_f$ where I denotes the set of indices $i \in \{1, \dots, r\}$ that appear in (3.7).

Let $v_{\nu j} = \mathrm{lcm}(v_{g_\nu}, v_{g_j})$ and $\tau_{\nu j} = \frac{v}{v_{\nu j}}$ for any $\nu, j \in I$, $\nu \ne j$. (Since $v = v_{H_i} v_{g_i}$ for every $i \in I$, $v_{g_\nu} \,|\, v$ and $v_{g_j} \,|\, v$, hence $v_{\nu j} \,|\, v$.) By Proposition 3.13, there exist elements $c_{\nu j} \in K$ $(1 \le \nu \le s, 1 \le j \le t$ for some $s, t \in \mathbb{N})$ such that

$$\tilde{f} = \sum_{\nu=1}^{s} \sum_{j=1}^{t} c_{\nu j} \tau_{\nu j} S_v(g_\nu, g_j), \tag{3.8}$$

and

$$\tau_{\nu j} v_{S_v(g_\nu, g_j)} = v_{\tau_{\nu j} S_v(g_\nu, g_j)} > v,\ \tau_{\nu j} u_{S_v(g_\nu, g_j)} \le u_{\tilde{f}} \tag{3.9}$$

$(1 \le \nu \le s, 1 \le j \le t)$. Since for any $i, j \in \{1, \dots, r\}$, $i \ne j$, $S_v(g_i, g_j) \xrightarrow[E^*]{G} 0$, there exist $q_{i\nu j} \in \mathfrak{D}$ $(1 \le i \le r)$ such that $S_v(g_\nu, g_j) = \sum_{i=1}^{r} q_{i\nu j} g_i$ where $v_{q_{i\nu j}} v_{g_i} \ge v_{S_v(g_\nu, g_j)}$ and $u_{q_{i\nu j}} u_{g_i} \le u_{S_v(g_\nu, g_j)}$ (see Theorem 3.10). Thus, for any indices ν and j in the sum (3.8), we have $\tau_{\nu j} S_v(g_\nu, g_j) = \sum_{i=1}^{r} (\tau_{\nu j} q_{i\nu j}) g_i$ where $v_{\tau_{\nu j} q_{i\nu j}} v_{g_i} = \tau_{\nu j} v_{q_{i\nu j}} v_{g_i} \ge \tau_{\nu j} v_{S_v(g_\nu, g_j)} > v$.

Setting $\tilde{H}_i = \sum_{\nu=1}^{s} \sum_{j=1}^{t} c_{\nu j} \tau_{\nu j} q_{i\nu j}$ $(1 \le i \le r)$, we obtain that

$$\tilde{f} = \sum_{\nu=1}^{s} \sum_{j=1}^{t} c_{\nu j} \sum_{i=1}^{r} (\tau_{\nu j} q_{i\nu j}) g_i = \sum_{i=1}^{r} \tilde{H}_i g_i \tag{3.10}$$

where $v_{\tilde{H}_i} v_{g_i} > v$ and $u_{\tilde{H}_i} u_{g_i} \le \max\{\tau_{\nu j} u_{q_{i\nu j}} u_{g_i} \,|\, 1 \le \nu \le s, 1 \le j \le t\} \le \max\{\tau_{\nu j} u_{S_v(g_\nu, g_j)} \,|\, 1 \le \nu \le s, 1 \le j \le t\} \le u_{\tilde{f}}$ (see (3.9)).

Substituting (3.10) into (3.6) we get

$$f = \sum_{i=1}^{r} \tilde{H}_i g_i + \sum_{v_{H_i} v_{g_i} = v} (H_i - d_i v_{H_i}) g_i + \sum_{v_{H_i} v_{g_i} > v} H_i g_i. \tag{3.11}$$

Let I_1, I_2 and I_3 be sets of indices for terms in the first, second and third sums in (14), respectively. Setting $H_i' = H_i - d_i v_{H_i}$ for every $i \in I_2$ we obtain that $v_{\tilde{H}_i} v_{g_i} > v$ for every $i \in I_1$, $v_{H_i'} v_{g_i} > v$ for every $i \in I_2$, and $v_{H_i} v_{g_i} > v$ for every $i \in I_2$. Furthermore, the inequality $u_{\tilde{H}_i} u_{g_i} \le u_{\tilde{f}}$ $(i \in I_1)$ implies that $u_{\tilde{H}_i} u_{g_i} \le u_f$. Also, if $i \in I_2$, then $u_{H_i'} u_{g_i} \le u_{H_i} u_{g_i} \le u_f$, and if $i \in I_3$, then $u_{H_i} u_{g_i} \le \max\{u_{H_i} u_{g_i} \,|\, 1 \le i \le r\} = u_f$. Thus, (3.11) is a representation of f in the form (3.4) with condition (3.5). We have arrived at a contradiction with the choice of the representation (3.4)

with condition (3.5) and the greatest possible term $v = \min\{v_{H_i} v_{g_i} \mid 1 \leq i \leq r\}$. thus, every $f \in N$ can be represented in the form (3.2) with conditions (3.3). □

The last theorem leads to the following Buchberger-type algorithm for constructing an E-Gröbner basis of a $\mathfrak{D}$-submodule N of F starting with a standard Gröbner basis. Its termination follows from the fact that every time when the algorithm requires adding a new element to G^*, we obtain a larger set where every two elements are E-reduced with respect to each other. As it follows from Remarks 3.4 and 3.11, this process of adding new elements to G^* must terminate, resulting in an E-Gröbner basis of N.

Algorithm II. $(r, g_1, \ldots, g_r;\ g_1^*, \ldots g_s^*)$
Input: $G = \{g_1, dots, g_r\}$ $(r \in \mathbb{N}, r > 0)$, *a standard Gröbner basis of a* $\mathfrak{D}$-submodule N of F **Output:** $G^* = \{g_1^*, \ldots g_s^*\}$, *an E-Gröbner basis of N*
Begin
$G^* := G$, $\mathfrak{U} := \{\{g_i, g_j\} \mid g_i \neq g_j \in G^*\}$
While $\mathfrak{U} \neq \emptyset$ **do**
Choose any $\{f, g\} \in \mathfrak{U}$
$\mathfrak{U} := \mathfrak{U} - \{\{f, g\}\}$
$S_v(f, g) \xrightarrow[E^*]{G^*} h$ *where h is E-reduced with respect to G^**
If $h \neq 0$, **then**
$h \xrightarrow[E]{G^*} h^*$
$\mathfrak{U} := \mathfrak{U} \cup \{\{t, h^*\} \mid t \in G^*\}$, $G^* := G^* \cup \{h^*\}$.
End

4. Bivariate Difference Dimension Polynomials

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ and M a finitely generated σ-K-module with generators $x_1, \ldots, x_n$ (that is, $M = \sum_{i=1}^n \mathfrak{D} x_i$ where $\mathfrak{D}$ is the ring of σ-operators over K). For any $r, s \in \mathbb{N}$, let $M_{rs} = \sum_{i=1}^n \mathfrak{D}_{rs} x_i$ where $\mathfrak{D}_{rs}$ denotes the K-vector subspace of $\mathfrak{D}$ generated by all elements $\tau \in T(r, s)$. Furthermore, let F be a free $\mathfrak{D}$-module with a basis $f_1, \ldots, f_n$, and $\pi : F \longrightarrow M$ the natural $\mathfrak{D}$-epimorphism of F onto M ($\pi(f_i) = x_i$ for $i = 1, \ldots, n$). Let $N = \operatorname{Ker} \pi$ and let $G = \{g_1, \ldots, g_p\}$ be an E-Gröbner basis of N. Let u_i and v_i denote the leader and coleader of g_i, respectively $(1 \leq i \leq p)$, and for any $r, s \in \mathbb{N}$ such that $s \leq r$, let $Tf = \{\tau f_i \mid \tau \in T, 1 \leq i \leq m\}$ and

$W(r, s) = \{w \in Tf \mid s \leq \operatorname{ord} w \leq r\}$, $W_M(r, s) = \pi(W(r, s))$,

$U'(r, s) = \{u \in Tf \mid s \leq \operatorname{ord} u \leq r$ and $u_i \nmid u\, (i = 1, \ldots, p)\}$, $U'_M(r, s) = \{\pi(u) \mid u \in U'(r, s)\}$,

$U''(r, s) = \{u \in Tf \mid s \leq \operatorname{ord} u \leq r$, u is divisible by some u_i $(1 \leq i \leq p)$ and whenever $u = \tau u_i$, for some $\tau \in T$ one has $\operatorname{ord}(\tau v_i) < s\}$, and $U''_M(r, s) = \{\pi(u) \mid u \in U''(r, s)\}$.

Furthermore, let $U(r, s) = U'(r, s) \bigcup U''(r, s)$ and $U_M(r, s) = U'_M(r, s) \bigcup U''_M(r, s)$.

Proposition 4.1. *With the above notation, let $s_0 = \max\{\operatorname{Eord} g_i \mid 1 \leq i \leq p\}$. Then for every $(r, s) \in \mathbb{N}^2$, $s \leq r - s_0$, the set $U_M(r, s)$ is a basis of the K-vector space M_{rs}.*

Proof. First, we are going to show that the set $U_M(r, s)$ $(s \leq r - s_0)$ is linearly independent over K. Let $\sum_{i=1}^k a_i \pi(w_i) = 0$ for some elements $w_1, \ldots, w_k \in U(r, s)$ and $a_1, \ldots, a_k \in K$. Then $h = \sum_{i=1}^k a_i w_i$ is an element of N which is E-reduced with respect to G. Indeed, if a term $w = \tau f_j$ appears in h (so that $w = w_i$ for some i, $1 \leq i \leq k$), then either w is not a transform of any u_ν

($1 \leq \nu \leq p$) or $w = \tau u_\nu$ for some $\tau \in T$, $1 \leq \nu \leq p$, such that $\mathrm{ord}(\tau v_\nu) < s \leq \mathrm{ord}\, v_h$, hence $\tau v_\nu < v_h$. Thus, h is E-reduced with respect to the E-Gröbner basis of G, hence (see Theorem 3.10) $h = 0$ and $a_1 = \cdots = a_k = 0$.

Now let us prove that if $s \in \mathbb{N}$ and $s \leq r - s_0$, then every element $\tau x_j \in W_M(r,s) \setminus U_M(r,s)$ ($\tau \in T$, $1 \leq j \leq n$) is a finite linear combination of elements of $U_M(r,s)$ with coefficients in K. Indeed, in this case $\tau f_j \notin U(r,s)$, hence $\tau f_j = \tau' u_i$ for some $\tau' \in T$ and $i \in \{1, \ldots, p\}$ such that $\mathrm{ord}(\tau' v_i) \geq s$. Let us consider the element $g_i = c_i u_i + \ldots$ ($c_i \in K, c_i \neq 0$), where dots are placed instead of the linear combination of terms that are less than u_i. Since $g_i \in N = \mathrm{Ker}\ \pi$, $\pi(g_i) = c_i \pi(u_i) + \cdots = 0$, whence $\pi(\tau' g_i) = c_j \pi(\tau' u_i) + \cdots = c_i \pi(\tau f_j) + \cdots = c_i \tau x_j + \cdots = 0$, so that τx_j is a finite linear combination with coefficients in K of some elements $\tilde{\tau} x_l$ ($1 \leq l \leq n$) such that $\tilde{\tau} \in T(r,s)$ and $\tilde{\tau} f_l < \tau' u_i$. Applying the induction on the well-ordered set Tf, we obtain that every element τx_i ($\tau \in T(r,s)$, $1 \leq i \leq n$) is a finite linear combination of elements of the set $\pi(U(r,s))$ with coefficients in K. It follows that $U_M(r,s)$ is a basis of the K-vector space M_{rs}. $\square$

Proposition 4.1 implies the following result whose proof can be obtained by repeating the arguments of the proof of Theorem 4.1 of [11] (and using Theorem 3.10 instead of Proposition 3.13 of [11]).

Theorem 4.2. *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ and M a finitely generated σ-K-module with generators $x_1, \ldots, x_n$ (that is, $M = \sum_{i=1}^n \mathfrak{D} x_i$ where $\mathfrak{D}$ is the ring of difference (σ-) operators over K). For any $r, s \in \mathbb{N}$, let $M_{rs} = \sum_{i=1}^n \mathfrak{D}_{rs} x_i$ where $\mathfrak{D}_{rs}$ denotes the K-vector subspace of $\mathfrak{D}$ generated by all elements τx_i ($1 \leq i \leq n$) with $\tau \in T(r,s)$. Then there exists a polynomial $\psi(t_1, t_2) \in \mathbb{Q}[t_1, t_2]$ and numbers $r_0, s_0, s_1 \in \mathbb{N}$ with $s_1 < r_0 - s_0$ such that*

(i) $\psi(r,s) = \dim_K M_{rs}$ *for all* $(r,s) \in \mathbb{N}^2$ *with* $r \geq r_0$, $s_1 \leq s \leq r - s_0$.

(ii) $\psi(t_1, t_2) = \psi^{(1)}(t_1) - \psi^{(2)}(t_2)$ *where* $\deg\, \psi^{(i)}(t) \leq m$ *($i = 1, 2$), so*

$$\psi_(t_1, t_2) = \sum_{i=0}^m a_i \binom{t_1 + i}{i} - \sum_{j=0}^m b_j \binom{t_2 + j}{j} \quad \textit{where } a_i, b_j \in \mathbb{Z}.$$

(iii) *For all sufficiently large $r \in \mathbb{N}$, $\psi^{(1)}(r) = \phi(r)$ where $\phi(t)$ is the difference (σ-) dimension polynomial of M associated with the filtration $(M_r = \sum_{i=1}^n \mathfrak{D}_r x_i)_{r \in \mathbb{Z}}$ where $\mathfrak{D}_r$ denotes the K-vector subspace of $\mathfrak{D}$ generated by all elements τx_i ($1 \leq i \leq n$) with $\tau \in T(r)$.*

(iv) $a_m = b_m = \sigma\text{-}\dim_K M$. *Furthermore, $d = \deg_{t_1} \psi$, and a_d are invariants of the σ-K-module M, that is, they do not depend on the finite system of σ-generators of M over K the polynomial $\psi(t_1, t_2)$ is associated with.*

(v) $\deg \psi^{(1)} \geq \deg \psi^{(2)}$ *and if* $\deg \psi^{(1)} = \deg \psi^{(2)} = e < m$, *then b_e is an invariant of M.*

Definition 4.3. The bivariate numerical polynomial $\psi(t_1, t_2)$ whose existence is established by Theorem 4.2 is called a σ-E-dimension polynomial of the σ-K-module M associated with the system of σ-K-generators $\{x_1, \ldots, x_n\}$.

Note that the presented E-Gröbner basis method gives an algorithm for computing σ-E-dimension polynomials while [11] give just an existence theorem. The following example shows that a σ-E-dimension polynomial $\psi_M(t_1, t_2)$ of a finitely generated σ-K-module M can carry more invariants (i. e., numbers that do not depend on the set of generators of M over $\mathfrak{D}$ the polynomial $\psi_M(t_1, t_2)$ is associated with) than the univariate difference dimension polynomial introduced in [6] and studied in [5], [9] and many other works (see Theorem 2.1).

Example 4.4. Let K be a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ and let M be a σ-K-module with two generators x_1 and x_2 (as a module over the ring of σ-operators $\mathfrak{D}$) and with the system of defining equations

$$\alpha_1^a x_1 + \alpha_2^{a-b} x_2 = 0 \qquad \text{and} \qquad \alpha_1^{a+b} x_2 + \alpha_2^{a-b} x_2 = 0 \tag{4.1}$$

where a and b are positive integers, $a > b \geq 1$. In other words, if F denotes the free $\mathfrak{D}$-module with free generators f_1 and f_2 and $g_1 = \alpha_1^a f_1 + \alpha_2^{a-b} f_2$, $g_2 = \alpha_1^{a+b} f_2 + \alpha_2^{a-b} f_2$, then $N = [g_1, g_2]$ is the kernel of the natural epimorphism of $\mathfrak{D}$-modules $F \to M$ ($f_1 \mapsto x_1$, $f_2 \mapsto x_2$). Since $u_{g_1} = \alpha_1^a f_1$ and $u_{g_2} = \alpha_1^{a+b} f_2$, $\mathrm{lcm}(u_{g_1}, u_{g_2}) = 0$, the standard S-polynomial of g_1 and g_2 (in the sense of [5, Chapter 4]) is 0, so $\{g_1, g_2\}$ is a "standard" Gröbner basis of N. Now, $v_{g_1} = v_{g_2} = \alpha_2^{a-b} f_2$, so $S_v(g_1, g_2) = g_2 - g_1 = \alpha_1^{a+b} f_2 - \alpha_1^a f_1$. We see that the least common multiples of the coleader $\alpha_1^a f_1$ of the element $g_3 = g_2 - g_1$ and coleaders of g_1 and g_2 are zeros, hence $G = \{g_1, g_2, g_3\}$ is an E-Gröbner basis of N. (Note that $\{g_1, g_2\}$ is not an E-Gröbner basis of N, since the element $g_3 \in N$ is E-reduced with respect to $\{g_1, g_2\}$: $u_{g_2} \,|\, u_{g_3}$, but $\frac{u_{g_3}}{u_{g_2}} v_{g_2} = \alpha_2^{a-b} f_2 < v_{g_3} = \alpha_1^a f_1$.)

Using the notation introduced at the beginning of this section (with $u_{g_1} = \alpha_1^a f_1$, $u_{g_2} = u_{g_3} = \alpha_1^{a+b} f_2$, $v_{g_1} = v_{g_2} = \alpha_2^{a-b} f_2$, and $v_{g_3} = \alpha_1^a f_1$), we obtain that if s is sufficiently large and $s \leq r - 2b$, then

$$U'(r,s) = \{u = \alpha_1^k \alpha_2^l f \in Tf \,|\, s \leq k + l \leq r,\ u_{g_i} \nmid u\ (i = 1, 2, 3)\}.$$

Using the notation of Section 2 and Theorem 2.4, we get

$$\mathrm{Card}\, U'(r,s) = \left[\mathrm{Card}\, V_{\{(a,0)\}}(r) - \mathrm{Card}\, V_{\{(a,0)\}}(s-1)\right] + \left[\mathrm{Card}\, V_{\{(a+b,0)\}}(r) - \mathrm{Card}\, V_{\{(a+b,0)\}}(s-1)\right] = \left[\binom{r+2}{2} - \binom{r+2-a}{2}\right] - \left[\binom{s+1}{2} - \binom{s+1-a}{2}\right] + \left[\binom{r+2}{2} - \binom{r+2-(a+b)}{2}\right] - \left[\binom{s+1}{2} - \binom{s+1-(a+b)}{2}\right] = (2a+b)r - (2a+b)s - b,$$

$$U''(r,s) = \{\alpha_1^k \alpha_2^l \alpha_1^a f_1 \,|\, s \leq k + l + a \leq r,\ \mathrm{ord}(\alpha_1^k \alpha_2^l \alpha_2^{a-b} f_2) < s\} \bigcup \{\alpha_1^k \alpha_2^l \alpha_1^{a+b} f_2 \,|\, s \leq k + l + a + b \leq r,\ \mathrm{ord}(\alpha_1^k \alpha_2^l \alpha_2^{a-b} f_2) < s\} \bigcup \{\alpha_1^k \alpha_2^l \alpha_1^{a+b} f_2 \,|\, s \leq k + l + a + b \leq r,\ \mathrm{ord}(\alpha_1^k \alpha_2^l \alpha_1^a f_1) < s\}.$$

Therefore, $\mathrm{Card}\, U''(r,s) = \mathrm{Card}\{(k,l) \in \mathbb{N}^2 \,|\, s - a \leq k + l < s - (a-b)\} + \mathrm{Card}\{(k,l) \in \mathbb{N}^2 \,|\, s - (a+b) \leq k + l < s - (a-b)\} = \left[\binom{s-(a-b)+1}{2} - \binom{s-a+1}{2}\right] + \left[|D\binom{s-(a-b)+1}{2} - \binom{s-(a+b)+1}{2}\right] = 3bs + \frac{1}{2}(b^2 - 4ab - 2a + b)$. It follows that

$$\mathrm{Card}\, U(r,s) = \mathrm{Card}\, U'(r,s) + \mathrm{Card}\, U''(r,s) = (2a+b)r - (2a-2b)s + \tfrac{1}{2}(b^2 - 4ab - 2a - b),$$

so the σ-E-dimension polynomial of M associated with the generators x_1 and x_2 and defining system (4.1) is as follows:

$$\psi(t_1, t_2) = (2a+b)t_1 - (2a-2b)t_2 + \frac{1}{2}(b^2 - 4ab - 2a - b).$$

Since $\{g_1, g_2\}$ is a "standard" Gröbner basis of N and leaders of g_1 and g_2 are $\alpha_1^a f_1$ and $\alpha_1^{a+b} f_2$, respectively, the "classical" univariate difference dimension polynomial $\phi(t)$ associated with the generators x_1 and x_2 and defining system (4.1) is

$$\phi(t) = \omega_{\{(a,0)\}}(t) + \omega_{\{(a+b,0)\}}(t) = \left[\tbinom{t+2}{2} - \tbinom{t+2-a}{2}\right] + \left[\tbinom{t+2}{2} - \tbinom{t+2-(a+b)}{2}\right] = (2a+b)t - \tfrac{1}{2}(2a^2 + 2ab + b^2 - 6a - 3b).$$

(see [5, Theorem 4.3.5]; as before, $\omega_A(t)$ denotes the Kolchin polynomial of a set $A \subset \mathbb{N}^2$).

The invariants of $\phi(t)$ are its degree 1 and the leading coefficient $2a + b$ (see Theorem 2.1). At the same time, $\psi(t_1, t_2)$ carries three such invariants: $\deg_{t_1} \psi = 1$, $2a + b$ (the coefficient of t_1), and $2a - 2b$ (the coefficient of t_2). Thus, $\psi(t_1, t_2)$ gives both parameters a and b of the defining system (4.1) while $\phi(t)$ gives just the sum of the parameters.

The following example illustrates an important application of the obtained results to the isomorphism problem for difference modules. It shows that two non-isomorphic finitely generated σ-K-modules can have the same set of invariants carried by their univariate difference dimension polynomials, but different sets of invariants carried by their σ-E-dimension polynomials. Thus,the fact that two σ-K-modules are not isomorphic can be proved by comparing the corresponding σ-E-dimension polynomials computed via the E-Gröbner basis method (while the test based on consideration of univariate dimension polynomials is inconclusive).

Example 4.5. With the assumption of Example 4.4, let M' be a σ-K-module with two generators z_1 and z_2 over the ring of σ-operators $\mathfrak{D}$ and with the system of defining equations

$$\alpha_2^{a+b} z_2 + \alpha_1^a z_1 = 0 \qquad \text{and} \qquad \alpha_1^a z_1 + \alpha_1^b z_2 = 0 \tag{4.2}$$

(a and b are positive integers, $a > b \geq 1$). If F is the free $\mathfrak{D}$-module with free generators f_1 and f_2 and $h_1 = \alpha_2^{a+b} f_2 + \alpha_1^a f_1$, $h_2 = \alpha_1^a f_1 + \alpha_1^b f_2$, then $M' \cong F/N$ where $N = [h_1, h_2]$ is the kernel of the natural epimorphism of $\mathfrak{D}$-modules $F \to M'$ ($f_1 \mapsto z_1$, $f_2 \mapsto z_2$). Here $u_{h_1} = \alpha_2^{a+b} f_2$, $u_{h_2} = \alpha_1^a f_1$, $v_{h_1} = \alpha_1^a f_1$, and $v_{h_2} = \alpha_1^b f_2$, so $\mathrm{lcm}(u_{h_1}, u_{h_2}) = 0$ and $S_v(h_1, h_2) = 0$. It follows that $\{h_1, h_2\}$ is an E-Gröbner basis of N. Proceeding as in Example 4.4, we obtain that the σ-E-dimension polynomial and the univariate difference dimension polynomial of M' associated with the generators z_1, z_2 and the defining system (4.2) are $\psi^*(t_1, t_2) = (2a+b)t_1 - (a+b)t_2 + \frac{1}{2}(2b^2 - a^2 + 5a)$ and $\phi^*(t) = (2a+b)t - \frac{1}{2}(2a^2 + 2ab + b^2 - 6a - 3b)$, respectively. We see that in this case the univariate difference dimension polynomial is the same as the corresponding dimension polynomial for module M in Example 4.4. At the same time, the σ-E-dimension polynomials of M and M' show that these σ-K-modules are not isomorphic, since the coefficients of t_2 in these polynomials are different ($2b - 2a$ and $-a - b$, respectively).

As it is shown in [11], Theorem 4.2 implies the following result for difference field extensions.

Theorem 4.6. *Let $L = K\langle \eta_1, \ldots, \eta_n \rangle$ be a σ-field extension generated by a set $\eta = \{\eta_1, \ldots, \eta_n\}$. (As before, $\sigma = \{\alpha_1, \ldots, \alpha_m\}$.) Then there exists a polynomial $\psi_{\eta|K}(t_1, t_2) \in \mathbb{Q}[t_1, t_2]$ and $r_0, s_0, s_1 \in \mathbb{N}$ with $s_1 < r_0 - s_0$ such that*

(i) $\psi_{\eta|K}(r, s) = \mathrm{tr.deg}_K\, K(\{\tau\eta_j \mid \tau \in T(r, s), 1 \leq j \leq n\})$ *for all $(r, s) \in \mathbb{N}^2$ with $r \geq r_0$, $s_1 \leq s \leq r - s_0$.*

(ii) $\psi_{\eta|K}(t_1, t_2) = \psi^{(1)}_{\eta|K}(t_1) - \psi^{(2)}_{\eta|K}(t_2)$ *where* $\deg\, \psi^{(i)}_{\eta|K}(t) \leq m$ *($i = 1, 2$), so $\psi_{\eta|K}(t_1, t_2)$ can be written as*

$$\psi_{\eta|K}(t_1, t_2) = \sum_{i=0}^{m} a_i \binom{t_1 + i}{i} - \sum_{j=0}^{m} b_j \binom{t_2 + j}{j}, \quad \textit{where } a_i, b_j \in \mathbb{Z}.$$

(iii) $a_m = b_m = \sigma\text{-tr.deg}_K\, L$. *Furthermore, $d = \deg_{t_1}\, \psi_{\eta|K}$, and a_d are also invariants of the extension L/K (they do not depend on the system of σ-generators of L/K). Finally,* $\deg \psi^{(1)}_{\eta|K} \geq \deg \psi^{(2)}_{\eta|K}$ *and if* $\deg \psi^{(1)}_{\eta|K} = \psi^{(2)}_{\eta|K} = e < m$, *then b_e is an invariant of the extension as well.*

The polynomial $\psi_{\eta|K}(t_1, t_2)$ is called a *σ-E-dimension polynomial* of the σ-field extension L/K associated with the system of σ-generators η. As it is shown in the proof of Theorem 4.5 of [11], $\psi_{\eta|K}(t_1, t_2)$ coincides with the σ-E-dimension polynomial of the σ-L-module of Kähler differentials associated with the extension L/K, so it can be computed via the E-Gröbner basis method.

Suppose that we have two systems of difference (σ-) algebraic equations that are defining equations of finitely generated σ-field extensions L/K and L'/K (it means that they generate prime reflexive σ-ideals P and P' of the ring of difference (σ-) polynomials $R = K\{y_1, \ldots, y_n\}$, respectively, such that L and L' are σ-isomorphic to the quotient fields of R/P and R/P', respectively). These systems are said to be *equivalent* if there is a σ-isomorphism between L and L' which is

identity on K. The last theorem allows one to use σ-E-dimension polynomials to figure out that two systems of σ-algebraic equations whose corresponding σ-field extensions have the same univariate σ-dimension polynomial are not equivalent. Say, two systems of algebraic difference equations $\alpha_1^a y_1 + \alpha_2^{a-b} y_2 = 0$, $\alpha_1^{a+b} y_2 + \alpha_2^{a-b} y_2 = 0$ and $\alpha_2^{a+b} y_2 + \alpha_1^a y_1 = 0$, $\alpha_1^a y_1 + \alpha_1^b z_2 = 0$, which correspond to the systems of equations on generators in Examples 4.4 and 4.5, define difference field extensions with the same univariate σ-dimension polynomial, but their σ-E-dimension polynomial are different and carry different invariants. Therefore the systems are not equivalent.

References

[1] Cohn, R. M. *Difference Algebra*. Interscience, New York, 1965.

[2] A. Einstein. The Meaning of Relativity. *Appendix II (Generalization of gravitation theory)*. Princeton University Press, Princeton, NJ, 1953, 153–165.

[3] M. Insa, and F. Pauer. Gróbner Bases in Rings of Differential Operators. Gröbner Bases and Applications, Cambridge Univ. Press, 1998, 367–380.

[4] E. R. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, 1973.

[5] M. V. Kondrateva, A. B. Levin, A. V. Mikhalev, and E. V. Pankratev. *Differential and Difference Dimension Polynomials*. Kluwer Acad. Publ., 1999.

[6] A. B. Levin. Characteristic Polynomials of Filtered Difference Modules and of Difference Field Extensions. *Russian Math. Surveys*, 33 (1978), no.3, 165–166.

[7] A. B. Levin. Computation of the Strength of Systems of Difference Equations via Generalized Gröbner Bases. *Grobner Bases in Symbolic Analysis*, Walter de Gruyter, 2007, 43–73.

[8] A. B. Levin. Gröbner Bases with Respect to Several Orderings and Multivariable Dimension Polynomials. *J. Symbolic Comput.*, 42 (2007), 561–578.

[9] A. B. Levin. *Difference Algebra*. Springer, 2008.

[10] A. B. Levin. Dimension polynomials of difference local algebras. *Advances in Applied Mathematics*, 72 (2016), 166 – 174.

[11] A. Levin. Reduction with Respect to the Effective Order and a New Type of Dimension Polynomials of Difference Modules. *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation (ISSAC '22)*, ACM, New York, 55–62.

[12] A. B. Levin and A. V. Mikhalev. Dimension Polynomials of Filtered Differential G-modules and Extensions of Differential G-fields. Contemporary Mathematics, 131 (1992), Part 2, 469–489.

[13] A. B. Levin and A. V. Mikhalev. Dimension Polynomials of Difference-Differential Modules and of Difference-Differential Field Extensions. *Abelian groups and Modules*, 10 (1995), 56–82.

[14] A. B. Levin and A. V. Mikhalev. Type and Dimension of Finitely Generated G-algebras. *Contemporary Mathematics*, 184 (1995), 275–280.

[15] T. Oaku and T. Shimoyama. A Gröbner Basis Method for Modules over Rings of Differential Operators. *J. Symbolic Comput.*, 18, (1994), 223–248.

[16] M. Zhou and F. Winkler. Gröbner Bases in Difference-Differential Modules. *Proc. of ISSAC*, 2013, 267–274. In *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (ISSAC '06)*, ACM, New York, 353–360.

[17] M. Zhou and F. Winkler. Computing Difference-Differential Dimension Polynomials by Relative Gröbner Bases in Difference-Differential Modules *J. Symbolic Comput.*, 43 (2008), 726–745.

Alexander Levin
Department of Mathematics
The Catholic University of America
Washington DC
20064 U.S.A.
e-mail: `levin@cua.edu`