Gröbner Bases in Difference-Differential Modules

Meng Zhou
Department of Mathematics and LMIB
Beihang University
Beijing(100083), China
zhoumeng1613@hotmail.com

Franz Winkler
Research Institute for Symbolic Computation
Johannes Kepler University Linz
A-4040, Linz, Austria
Franz.Winkler@jku.at

ABSTRACT

We extend the theory of Gröbner bases to difference-differential modules. The main goal of this paper is to present and verify algorithms for constructing Gröbner bases for such difference-differential modules. To this aim we introduce the concept of generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ and on difference-differential modules.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*Algebraic algorithms*

General Terms

Algorithms

Keywords

Gröbner basis, difference and differential operators

1. INTRODUCTION

The usefulness of the classical Gröbner basis method for the algorithmic solution of problems in polynomial ideal theory is well-known. The results of Buchberger [2], [3] on Gröbner bases in polynomial rings have been extensively described, for instance by Becker and Weispfenning [1], Cox et al. [4], and Winkler [14]. The theory has been generalized by many authors to non-commutative domains, especially to modules over various rings of differential operators. Galligo [5] first gave the Gröbner basis algorithm for the Weyl algebra $\mathcal{A}_m(K)$ of partial differential operators with coefficients in a polynomial ring over the field K. Mora [9] generalized the concept of Gröbner basis to non-commutative free algebras. Kondrateva et al. [7] described the Gröbner basis method for differential and difference modules. Noumi [10] and Takayama [13] formulated Gröbner bases in R_n, the ring of differential operators with rational function coefficients. Oaku and Shimoyama [11] treated D_0, the ring of differential operators with power series coefficients. Insa and Pauer [6] presented a basic theory of Gröbner bases for differential operators with coefficients in a commutative Noetherian ring. It has been proved that the notion of Gröbner basis is a powerful tool to solve various problems of linear partial differential equations.

On the other hand, for some problems of linear difference-differential equations such as the dimension of the space of solutions and the computation of difference-differential dimension polynomials, the notion of Gröbner basis for the ring of difference-differential operators is essential. Whereas Gröbner bases in rings of differential operators are defined with respect to a term order on $\mathbb{N}^n \times \mathbb{N}^n$ or $\mathbb{N}^n$, this approach cannot be used for the ring of difference-differential operators. We need to treat orders on $\mathbb{N}^m \times \mathbb{Z}^n$. Pauer and Unterkircher [12] considered Gröbner bases in Laurent polynomial rings, but their approach is limited to the commutative case. Levin [8] introduced characteristic sets for free modules over rings of difference-differential operators. Such characteristic sets depend on a specific order on $\mathbb{N}^m \times \mathbb{Z}^n$. But this order is not a term order in the sense of the theory of Gröbner bases.

The main purpose of this paper is to give a new approach to the computation of a Gröbner basis for an ideal in (or a module over) the ring of difference-differential operators. Our notion of Gröbner basis is based on a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$. In Section 2 the generalized term order and its properties are discussed and some examples are presented. In Section 3 we introduce the reduction algorithm, the definition of the Gröbner basis and the S-polynomials, as well as the Buchberger algorithm for the computation of Gröbner bases. Further details can be found in [15].

Throughout the paper, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_+$, $\mathbb{Z}_-$ and $\mathbb{Q}$ denote the sets of natural numbers, integers, nonnegative integers (i.e. natural numbers), nonpositive integers, and rational numbers, respectively. By a ring we always mean an associative ring with a unit. By the module over a ring A we mean a unitary left A-module.

DEFINITION 1.1. *Let R be a commutative Noetherian ring. Let $\Delta = \{\delta_1, \cdots, \delta_m\}$ be a set of derivations on R and $\Sigma = \{\sigma_1, \cdots, \sigma_n\}$ a set of automorphisms of R, such that $\alpha(x) \in R$ and $\alpha(\beta(x)) = \beta(\alpha(x))$ for any $\alpha, \beta \in \Delta \cup \Sigma$ and $x \in R$. Then R is called a* difference-differential ring *with the basic set of derivations Δ and the basic set of automorphisms Σ, or shortly a* Δ-Σ-ring*; if R is a field, then it is called a* Δ-Σ-field.

This notion of difference-differential ring is motivated by the following example.

ISSAC'06, July 9–12, 2006, Genova, Italy.

Example 1.1. *Let* $R = K[x_1, \dots, x_n]$ *for a field* K, $\delta_i = \partial/\partial x_i$ *and* σ_i *the automorphism which maps* x_i *to* $x_i - 1$. *Then* R *is a* Δ-Σ-*ring for* $\Delta = \{\delta_1, \dots, \delta_n\}$ *and* $\Sigma = \{\sigma_1, \dots, \sigma_n\}$.

Let R be a Δ-Σ-ring. By Δ^* we denote the free commutative semigroup consisting of all words over Δ of the form $\delta_1^{k_1} \cdots \delta_m^{k_m}$, where $(k_1, \dots, k_m) \in \mathbb{N}^m$.

By $\tilde{\Sigma}$ we denote Σ together with its inverses, i.e. $\tilde{\Sigma} = \Sigma \cup \{\sigma^{-1} \mid \sigma \in \Sigma\}$. By Σ^* we denote the free commutative semigroup consisting of all words over Σ of the form $\sigma_1^{l_1} \cdots \sigma_n^{l_n}$, where $(l_1, \dots, l_n) \in \mathbb{N}^n$. By $\tilde{\Sigma}^*$ we denote the free commutative group consisting of all words over $\tilde{\Sigma}$ of the form $\sigma_1^{l_1} \cdots \sigma_n^{l_n}$, where $(l_1, \dots, l_n) \in \mathbb{Z}^n$.

By $\Lambda = (\Delta\tilde{\Sigma})^*$ we denote the free commutative semigroup consisting of all words over Δ and $\tilde{\Sigma}$ of the form

$$\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \sigma_1^{l_1} \cdots \sigma_n^{l_n}, \tag{1.1}$$

where $(k_1, \dots, k_m) \in \mathbb{N}^m$ and $(l_1, \dots, l_n) \in \mathbb{Z}^n$. Elements of Λ are called *terms*.

Definition 1.2. *Let* R *be a* Δ-Σ-*ring and the semigroup* Λ *be as above. Then an expression of the form*

$$\sum_{\lambda \in \Lambda} a_\lambda \lambda, \tag{1.2}$$

where $a_\lambda \in R$ *for all* $\lambda \in \Lambda$ *and only finitely many coefficients* a_λ *are different from zero, is called a* difference-differential operator *(or shortly a* Δ-Σ-operator*) over* R. *Two* Δ-Σ-*operators* $\sum_{\lambda \in \Lambda} a_\lambda \lambda$ *and* $\sum_{\lambda \in \Lambda} b_\lambda \lambda$ *are equal if and only if* $a_\lambda = b_\lambda$ *for all* $\lambda \in \Lambda$.

The set of all Δ-Σ-operators over a Δ-Σ-ring R is a ring with the following fundamental relations

$$\begin{array}{rcl} \sum_{\lambda\in\Lambda} a_\lambda\lambda + \sum_{\lambda\in\Lambda} b_\lambda\lambda & = & \sum_{\lambda\in\Lambda}(a_\lambda + b_\lambda)\lambda, \\ a(\sum_{\lambda\in\Lambda} a_\lambda\lambda) & = & \sum_{\lambda\in\Lambda}(aa_\lambda)\lambda, \\ (\sum_{\lambda\in\Lambda} a_\lambda\lambda)\mu & = & \sum_{\lambda\in\Lambda} a_\lambda(\lambda\mu), \\ \delta a = a\delta + \delta(a), & & \sigma a = \sigma(a)\sigma, \end{array} \tag{1.3}$$

for all $a_\lambda, b_\lambda \in R$, $\lambda, \mu \in \Lambda$, $a \in R$, $\delta \in \Delta$, $\sigma \in \tilde{\Sigma}$. Note that the elements in Δ and $\tilde{\Sigma}$ do not commute with the elements in R, and therefore the terms $\lambda \in \Lambda$ do not commute with the coefficients $a_\lambda \in R$.

Definition 1.3. *The ring of all* Δ-Σ-*operators over a* Δ-Σ-*ring* R *is called the* ring of difference-differential operators *(or shortly the* ring of Δ-Σ-operators*) over* R. *It will be denoted by* D. *A left* D-*module* M *is called a* difference-differential module *(or a* Δ-Σ-module*). If* M *is finitely generated as a left* D-*module, then* M *is called a finitely generated* Δ-Σ-*module.*

When $\Sigma = \emptyset$, D will be the ring of differential operators $R[\delta_1, \cdots, \delta_m]$. If the coefficient ring R is the polynomial ring in $x_1, \dots, x_m$ over a field K and $\delta_i = \partial/\partial x_i$ for $1 \le i \le m$, then D will be the Weyl algebra $\mathcal{A}_m(K)$. So Δ-Σ-modules are generalizations of modules over rings of differential operators. But in the ring of Δ-Σ-operators the terms are of the form (1.1) and the exponent in $\sigma_1, \cdots, \sigma_n$ is $(l_1, \cdots, l_n) \in \mathbb{Z}^n$. The notion of term order, as commonly used in Gröbner basis theory, is no longer valid. We need to generalize the concept of term order.

2. GENERALIZED TERM ORDER

First we consider decompositions of the group $\mathbb{Z}^n$.

Definition 2.1. *Let* $\mathbb{Z}^n$ *be the union of finitely many subsets* $\mathbb{Z}_j^n$, *i.e.* $\mathbb{Z}^n = \bigcup_{j=1}^k \mathbb{Z}_j^n$, *where* $\mathbb{Z}_j^n$, $j = 1, \cdots, k$, *satisfy the following conditions:*

(i) $(0, \cdots, 0) \in \mathbb{Z}_j^n$, *and* $\mathbb{Z}_j^n$ *does not contain any pair of invertible elements* $c = (c_1, \cdots, c_n) \ne 0$ *and* $-c = (-c_1, \cdots, -c_n)$,

(ii) $\mathbb{Z}_j^n$ *is isomorphic to* $\mathbb{N}^n$ *as a semigroup,*

(iii) the group generated by $\mathbb{Z}_j^n$ *is* $\mathbb{Z}^n$.

Then $\{\mathbb{Z}_j^n \mid j = 1, \cdots, k\}$ *is called an* orthant decomposition *of* $\mathbb{Z}^n$ *and* $\mathbb{Z}_j^n$ *is called the* j-th orthant *of the decomposition.*

Example 2.1. *Let* $\{\mathbb{Z}_1^n, \cdots, \mathbb{Z}_{2^n}^n\}$ *be all distinct Cartesian products of* n *sets each of which is either* $\mathbb{Z}_+$ *or* $\mathbb{Z}_-$. *Then this is an orthant decomposition of* $\mathbb{Z}^n$. *The set of generators of* $\mathbb{Z}_j^n$ *as a semigroup is*

$$\{(c_1, 0, \cdots, 0), (0, c_2, 0, \cdots, 0), \cdots, (0, \cdots, 0, c_n)\},$$

where c_j *is either* 1 *or* -1, $j = 1, \cdots, n$. *We call this decomposition the* canonical orthant decomposition *of* $\mathbb{Z}^n$.

Example 2.2. *Consider* $n \in \mathbb{N}$. *For* $i = 1, \dots, n$ *let*

$$z_i = (z_{i,j})_{1 \le j \le n}, \text{where } z_{i,j} = \begin{cases} 0 & \text{for } i \ne j \\ 1 & \text{for } i = j \end{cases}.$$

Furthermore let $z_0 = (z_{0,j})_{1 \le j \le n}$, *where* $z_{0,j} = -1$.

Let $\mathbb{Z}_0^n$ *be the sub-semigroup of* $\mathbb{Z}^n$ *generated by*

$$\{z_i \mid 1 \le i \le n\},$$

and for $1 \le j \le n$ *let* $\mathbb{Z}_j^n$ *be the sub-semigroup of* $\mathbb{Z}^n$ *generated by*

$$\{z_0\} \cup \{z_i \mid 1 \le i \le n \text{ and i} \ne \text{j}\}.$$

Then $\{\mathbb{Z}_0^n, \mathbb{Z}_1^n, \cdots, \mathbb{Z}_n^n\}$ *is an orthant decomposition of* $\mathbb{Z}^n$. *For* $n = 2$, *we have*

$$\mathbb{Z}_0^2 = \{(a, b) | a \ge 0, b \ge 0, a, b \in \mathbb{Z}\},$$

$$\mathbb{Z}_1^2 = \{(a, b) | a \le 0, b \ge a, a, b \in \mathbb{Z}\},$$

$$\mathbb{Z}_2^2 = \{(a, b) | b \le 0, a \ge b, a, b \in \mathbb{Z}\}.$$

Definition 2.2. *Let* $\{\mathbb{Z}_j^n \mid j = 1, \cdots, k\}$ *be an orthant decomposition of* $\mathbb{Z}^n$. *Then* $a = (k_1, \cdots, k_m, l_1, \cdots, l_n)$ *and* $b = (r_1, \cdots, r_m, s_1, \cdots, s_n)$ *of* $\mathbb{N}^m \times \mathbb{Z}^n$ *are called* similar *elements, if the* n-*tuples* $(l_1, \cdots, l_n)$ *and* $(s_1, \cdots, s_n)$ *are in the same orthant* $\mathbb{Z}_j^n$ *of* $\mathbb{Z}^n$.

Definition 2.3. *Let* $\{\mathbb{Z}_j^n \mid j = 1, \cdots, k\}$ *be an orthant decomposition of* $\mathbb{Z}^n$. *A total order* $\prec$ *on* $\mathbb{N}^m \times \mathbb{Z}^n$ *is called a* generalized term order *on* $\mathbb{N}^m \times \mathbb{Z}^n$ *w.r.t. the decomposition, if the following conditions hold:*

(i) $(0, \cdots, 0)$ *is the smallest elements in* $\mathbb{N}^m \times \mathbb{Z}^n$,

(ii) if $a \prec b$, *then* $a + c \prec b + c$ *for any* c *similar to* b.

EXAMPLE 2.3. *(a) Let* $\{\mathbb{Z}_j^n \mid j=1,\cdots,2^n\}$ *be the canonical orthant decomposition of* $\mathbb{Z}^n$ *defined in Example 2.1. For every* $a=(k_1,\cdots,k_m,l_1,\cdots,l_n)\in\mathbb{N}^m\times\mathbb{Z}^n$ *let*

$$|a| = k_1+\cdots+k_m+|l_1|+\cdots+|l_n|.$$

For two elements $a=(k_1,\cdots,k_m,l_1,\cdots,l_n)$ *and* $b=(r_1,\cdots,r_m,s_1,\cdots,s_n)$ *of* $\mathbb{N}^m\times\mathbb{Z}^n$ *define* $a\prec b$ *if and only if the* $(1+m+n)$*-tuple* $(|a|,k_1,\cdots,k_m,l_1,\cdots,l_n)$ *is smaller than* $(|b|,r_1,\cdots,r_m,s_1,\cdots,s_n)$ *w.r.t. the lexicographic order on* $\mathbb{N}^{m+1}\times\mathbb{Z}^n$*. Then "*$\prec$*" is a generalized term order on* $\mathbb{N}^m\times\mathbb{Z}^n$*.*
(b) Let the orthant decomposition of $\mathbb{Z}^n$ *be as in Example 2.1. For every* $a=(k_1,\cdots,k_m,l_1,\cdots,l_n)\in\mathbb{N}^m\times\mathbb{Z}^n$ *let*

$$|a|_1=\sum_{j=1}^m k_j, \qquad |a|_2=\sum_{j=1}^n |l_j|.$$

For two elements $a=(k_1,\cdots,k_m,l_1,\cdots,l_n)$ *and* $b=(r_1,\cdots,r_m,s_1,\cdots,s_n)$ *of* $\mathbb{N}^m\times\mathbb{Z}^n$ *define* $a\prec b$ *if and only if the* $(2+m+2n)$*-tuple*

$$(|a|_1,|a|_2,k_1,\cdots,k_m,|l_1|,\cdots,|l_n|,l_1,\cdots,l_n)$$

is lexicographically smaller than

$$(|b|_1,|b|_2,r_1,\cdots,r_m,|s_1|,\cdots,|s_n|,s_1,\cdots,s_n).$$

Then "$\prec$*" is a generalized term order on* $\mathbb{N}^m\times\mathbb{Z}^n$*.*
(c) Let $\{\mathbb{Z}_j^{(n)},\ j=0,1,\cdots,n\}$ *be the orthant decomposition of* $\mathbb{Z}^n$ *defined in Example 2.2. For every element* $a=(k_1,\cdots,k_m,l_1,\cdots,l_n)\in\mathbb{N}^m\times\mathbb{Z}^n$ *let*

$$\|a\| = -\min\{0,l_1,\cdots,l_n\}\ .$$

For two elements $a=(k_1,\cdots,k_m,l_1,\cdots,l_n)$ *and* $b=(r_1,\cdots,r_m,s_1,\cdots,s_n)$ *of* $\mathbb{N}^m\times\mathbb{Z}^n$ *define* $a\prec b$ *if and only if the* $(1+m+n)$*-tuple* $(\|a\|,k_1,\cdots,k_m,l_1,\cdots,l_n)$ *is lexicographically smaller than* $(\|b\|,r_1,\cdots,r_m,s_1,\cdots,s_n)$*. Then "*$\prec$*" is a generalized term order on* $\mathbb{N}^m\times\mathbb{Z}^n$*.*

In order to investigate Δ-Σ-modules, we need to extend the notion of generalized term order to $\mathbb{N}^m\times\mathbb{Z}^n\times E$, where $E=\{e_1,\cdots,e_q\}$ is a set of generators of a module.

DEFINITION 2.4. *Let* $\{\mathbb{Z}_j^n \mid j=1,\cdots,k\}$ *be an orthant decomposition of* $\mathbb{Z}^n$*. Let* $E=\{e_1,\cdots,e_q\}$ *be a set of* q *distinct elements. A total order* $\prec$ *on* $\mathbb{N}^m\times\mathbb{Z}^n\times E$ *is called a* generalized term order *on* $\mathbb{N}^m\times\mathbb{Z}^n\times E$ *w.r.t. the decomposition, if the following conditions hold:*

(i) $(0,\cdots,0,e_i)$ *is the smallest element in* $\mathbb{N}^m\times\mathbb{Z}^n\times\{e_i\}$ *for any* $e_i\in E$*,*

(ii) if $(a,e_i)\prec(b,e_j)$*, then* $(a+c,e_i)\prec(b+c,e_j)$ *for any* c *similar to* b*.*

There are many ways to extend a generalized term order on $\mathbb{N}^m\times\mathbb{Z}^n$ to $\mathbb{N}^m\times\mathbb{Z}^n\times E$. Of course such an extended term order may also be defined directly. Some typical examples are shown below.

EXAMPLE 2.4. *Let the orthant decomposition of* $\mathbb{Z}^n$ *and the generalized term order "*$\prec$*" on* $\mathbb{N}^m\times\mathbb{Z}^n$ *be as in Example 2.3(b). Given an order "*$\prec_E$*" on* $E=\{e_1,\cdots,e_q\}$*, for two elements*

$$\begin{aligned}(a,e_i) &= (k_1,\cdots,k_m,l_1,\cdots,l_n,e_i) \quad \text{and}\\ (b,e_j) &= (r_1,\cdots,r_m,s_1,\cdots,s_n,e_j)\end{aligned}$$

of $\mathbb{N}^m\times\mathbb{Z}^n\times E$ *define:*

$$(a,e_i)\prec_1(b,e_j) \iff a\prec b \quad \text{or} \quad (a=b \ \text{ and } \ e_i\prec_E e_j);$$

$$(a,e_i)\prec_2(b,e_j) \iff e_i\prec_E e_j \quad \text{or} \quad (e_i=e_j \ \text{ and } \ a\prec b);$$

$$\begin{aligned}(a,e_i)\prec_3(b,e_j) \iff & \\ &(|a|_1,|a|_2,e_i,k_1,\cdots,k_m,|l_1|,\cdots,|l_n|,l_1,\cdots,l_n)\\ &<(|b|_1,|b|_2,e_j,r_1,\cdots,r_m,|s_1|,\cdots,|s_n|,s_1,\cdots,s_n)\\ &\text{in lexicographic order.}\end{aligned}$$

Then "$\prec_1$*", "*$\prec_2$*","*$\prec_3$*" are generalized term orders on* $\mathbb{N}^m\times\mathbb{Z}^n\times E$*.*

We say that "$\prec_1$*" is the TOP (i.e.* term-over-position*) extension of "*$\prec$*" and "*$\prec_2$*" is the POT (i.e* position-over-term*) extension of "*$\prec$*". "*$\prec_3$*" is a generalized term order defined directly.*

LEMMA 2.1. *Let* $\{\mathbb{Z}_j^n \mid j=1,\cdots,k\}$ *be an orthant decomposition of* $\mathbb{Z}^n$ *and "*$\prec$*" be a generalized term order on* $\mathbb{N}^m\times\mathbb{Z}^n$ *with respect to the orthant decomposition. Then every strictly descending sequence in* $\mathbb{N}^m\times\mathbb{Z}^n$ *is finite. In particular, every subset of* $\mathbb{N}^m\times\mathbb{Z}^n$ *contains a smallest element.*

PROOF. Let $a_1\succ a_2\succ a_3\succ\cdots$ be a strictly descending sequence in $\mathbb{N}^m\times\mathbb{Z}^n$. Since there are finitely many orthants, without loss of generality we may assume that all a_j are similar elements, i.e. $a_j\in\mathbb{N}^m\times\mathbb{Z}_i^n$ for a fixed i. By Condition (ii) in Definition 2.1, $\mathbb{N}^m\times\mathbb{Z}_i^n$ is isomophic to $\mathbb{N}^{m+n}$ as a semigroup. Define order $\prec_1$ on $\mathbb{N}^{m+n}$ as follows:

$$a\prec_1 b \iff f^{-1}(a)\prec f^{-1}(b),$$

where f is the isomophism from $\mathbb{N}^m\times\mathbb{Z}_i^n$ to $\mathbb{N}^{m+n}$ and $\prec$ is the generalized term order on $\mathbb{N}^m\times\mathbb{Z}^n$. Since $\prec$ is a term order on $\mathbb{N}^m\times\mathbb{Z}_i^{(n)}$, it is easy to see $\prec_1$ is a term order (in the classical sense) on $\mathbb{N}^{m+n}$. Then the assertion of the Lemma follows from the well-order property of the term order on $\mathbb{N}^{m+n}$. $\Box$

COROLLARY 2.1. *Given an orthant decomposition of* $\mathbb{Z}^n$ *and a generalized term order "*$\prec$*" on* $\mathbb{N}^m\times\mathbb{Z}^n\times E$*, every strictly descending sequence in* $\mathbb{N}^m\times\mathbb{Z}^n\times E$ *is finite. In particular, every subset of* $\mathbb{N}^m\times\mathbb{Z}^n\times E$ *contains a smallest element.*

PROOF. Let $a_1\succ a_2\succ a_3\succ\cdots$ be a strictly descending sequence in $\mathbb{N}^m\times\mathbb{Z}^n\times E$. Since E is a finite set, we may suppose that all a_j are in $\mathbb{N}^m\times\mathbb{Z}^n\times\{e_i\}$ for a fixed i. Then the conclusion follows immediately from Lemma 2.1. $\Box$

3. GRÖBNER BASES IN FINITELY GENERATED DIFFERENCE-DIFFERENTIAL MODULES

Let $\{\mathbb{Z}_j^n \mid j=1,\cdots,k\}$ be an orthant decomposition of $\mathbb{Z}^n$ and "$\prec$" be a generalized term order on $\mathbb{N}^m\times\mathbb{Z}^n$ w.r.t. the ortant decomposition. Let Λ be the semi-group of terms introduced in Section 1 in which the elements are of the form (1.1). Since Λ is isomorphic to $\mathbb{N}^m\times\mathbb{Z}^n$ as a semigroup, the order "$\prec$" defines an order on Λ; we also call it a generalized term order on Λ.

Let K be a Δ-Σ-field and D be the ring of Δ-Σ-operators over K, and let F be a finitely generated free D-module (i.e. a finitely generated free difference-differential-module) with a set of free generators $E=\{e_1,\cdots,e_q\}$. Then F can be considered as a K-vector space generated by the set of all elements of the form λe_i, where $\lambda \in \Lambda$ and $i = 1, \ldots, q$. This set will be denoted by ΛE and its elements will be called "terms" of F. If "$\prec$" is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n \times E$ then "$\prec$" obviously induces an order on ΛE, which we also call a generalized term order.

It is clear that every element $f \in F$ has a unique representation as a linear combination of terms

$$f = a_1\lambda_1 e_{j_1} + \cdots + a_d\lambda_d e_{j_d} \tag{3.1}$$

for some nonzero elements $a_i \in K$ $(i = 1, \cdots, d)$ and some distinct elements $\lambda_1 e_{j_1}, \cdots, \lambda_d e_{j_d} \in \Lambda E$. If a term λe_j appears with nonzero coefficient in the representation (3.1) of f, then it is called a term of f. If $(k_1, \cdots, k_m, l_1, \cdots, l_n)$ and $(r_1, \cdots, r_m, s_1, \cdots, s_n)$ are similar elements in $\mathbb{N}^m \times \mathbb{Z}^n$ then the two terms $\lambda_1 = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n}$ and $\lambda_2 = \delta_1^{r_1} \cdots \delta_m^{r_m} \alpha_1^{s_1} \cdots \alpha_n^{s_n}$ in Λ are also called similar. If λ_1,$\lambda_2 \in \Lambda$ are similar, then the two terms $u = \lambda_1 e_i$ and $v = \lambda_2 e_j \in \Lambda E$ are also called similar.

Definition 3.1. *Let $\lambda_1 = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n}$ and $\lambda_2 = \delta_1^{r_1} \cdots \delta_m^{r_m} \alpha_1^{s_1} \cdots \alpha_n^{s_n}$ be two elements in Λ. If they are similar and $r_\mu \le k_\mu$, $|s_\nu| \le |l_\nu|$ for $\mu = 1, \cdots, m$, $\nu = 1, \cdots, n$, then λ_1 is called a* multiple *of λ_2 and this relation is denoted by $\lambda_2|\lambda_1$. If $\lambda_2|\lambda_1$ and $i = j$ then $u = \lambda_1 e_i$ is called a* multiple *of $v = \lambda_2 e_j$ and this relation is denoted by $v|u$.*

Definition 3.2. *Let $\prec$ be a generalized term order on ΛE, $f \in F$ be of the form (3.1). Then*

$$\mathrm{lt}(f) = \max_{\prec}\{\lambda_i e_{j_i} | i = 1, \cdots, d\}$$

is called the leading term *of f. If $\lambda_i e_{j_i} = \mathrm{lt}(f)$, then a_i is called the* leading coefficient *of f, denoted by $\mathrm{lc}(f)$.*

Now we are going to construct the division algorithm in the difference-differential module F. First we collect some properties of relating multiplication of terms to the ordering. In what follows we always assume that an orthant decomposition of $\mathbb{Z}^n$ is given as well as a generalized term order $\prec$ w.r.t. this decomposition.

Definition 3.3. *Let $\{\mathbb{Z}_j^n \mid j = 1, \ldots, k\}$ be an orthant decomposition of $\mathbb{Z}^n$. Then the subset Λ_j of Λ,*

$$\Lambda_j = \{\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n} \mid (l_1, \cdots, l_n) \in \mathbb{Z}_j^n\},$$

*is called the j-*th orthant *of Λ. Let F be a finitely generated free D-module and ΛE be the set of terms of F. Then*

$$\Lambda_j E = \{\lambda e_i \mid \lambda \in \Lambda_j, e_i \in E\}$$

*is called the j-*th orthant *of ΛE.*

Obviously, two elements in Λ or ΛE are similar if and only if they are in the same orthant. So from Definition 2.3, if $\prec$ is a generalized term order on Λ and $\xi \prec \lambda$, then $\eta\xi \prec \eta\lambda$ holds for any η in the same orthant as λ.

Lemma 3.1. *Let $\lambda \in \Lambda, a \in K$, and $\prec$ be a generalized term order on $\Lambda E \subseteq D$. Then*

$$\lambda a = a'\lambda + \xi,$$

where $a' = \sigma(a)$ for some $\sigma \in \Sigma^*$. If $a \ne 0$ then also $a' \ne 0$. Furthermore, $\xi \in D$ with $\mathrm{lt}(\xi) \prec \lambda$ and all terms of ξ are similar to λ.

Note that for a generalized term order $\prec$ we cannot expect $\lambda \mathrm{lt}(f) = \mathrm{lt}(\lambda f)$ unless the leading term $\mathrm{lt}(f) = \eta e_i$ of f is such that η is similar to λ.

Lemma 3.2. *Let F be a finitely generated free D-module and $0 \ne f \in F$. Then the following hold:*

(i) If $\lambda \in \Lambda$, then $\mathrm{lt}(\lambda f) = \lambda \cdot u$ for a unique term u of f.

(ii) If $\mathrm{lt}(f) \in \Lambda_j E$ then for any $\lambda \in \Lambda_j$

$$\mathrm{lt}(\lambda f) = \lambda \cdot \mathrm{lt}(f) \in \Lambda_j E.$$

Lemma 3.3. *Let F be a finitely generated free D-module and $0 \ne f \in F$. Then for each j, there exists some $\lambda \in \Lambda$ and a unique term u_j of f such that*

$$\mathrm{lt}(\lambda f) = \lambda \cdot u_j \in \Lambda_j E.$$

We will write $lt_j(f)$ for this term u_j.

If $h \in D$, $f \in F$, then $hf = \sum_{i,k} a_{i,k}\lambda_i u_k$ for some $\lambda_i \in \Lambda$ and $u_k \in \Lambda E$, some of which might not be terms of h and f. It would be problematic if $\mathrm{lt}(hf) \prec \lambda_i u_k$ might occur for some λ_i and u_k in hf. The following proposition asserts that this undesirable situation cannot occur.

Proposition 3.1. *Let $0 \ne f \in F$, $0 \ne h \in D$. Then $\mathrm{lt}(hf) = \max_\prec\{\lambda_i u_k\}$ where λ_i are terms of h and u_k are terms of f. Therefore $\mathrm{lt}(hf) = \lambda \cdot u$ for a unique term λ of h and a unique term u of f.*

Now we are ready to introduce the concept of "reduction", which is central in the theory of Gröbner bases.

Theorem 3.1. *Let $f_1, \cdots, f_p \in F \setminus \{0\}$. Then every $g \in F$ can be represented as*

$$g = h_1 f_1 + \cdots + h_p f_p + r \tag{3.2}$$

for some elements $h_1, \cdots, h_p \in D$ and $r \in F$ such that

(i) $h_i = 0$ or $\mathrm{lt}(h_i f_i) \preceq \mathrm{lt}(g)$ for $i = 1, \cdots, p$,

(ii) $r = 0$ or $\mathrm{lt}(r)$ is not a multiple of any $\mathrm{lt}(\lambda f_i)$ for $\lambda \in \Lambda$, $i = 1, \cdots, p$.

Proof. The elements $h_1, \cdots, h_p \in D$ and $r \in F$ can be computed as follows: first set $r = g$ and $h_i = 0$ for $i = 1, \ldots, p$. Suppose $r \ne 0$, i.e.

$$r = \mathrm{lc}(r)\mathrm{lt}(r) + \tilde{r},$$

and $\mathrm{lt}(r)$ is a multiple of $\mathrm{lt}(\lambda_i f_i)$ for an element $\lambda_i \in \Lambda$. Suppose $\mathrm{lt}(\lambda_i f_i) \in \Lambda_j E$. Then there exists an element $\eta \in \Lambda_j$ such that

$$\mathrm{lt}(r) = \eta \cdot \mathrm{lt}(\lambda_i f_i).$$

By Lemma 3.2.(ii), $\mathrm{lt}(\eta \cdot \lambda_i f_i) = \eta \cdot \mathrm{lt}(\lambda_i f_i) = \mathrm{lt}(r)$. So

$\eta \cdot \lambda_i f_i = c_i \eta \cdot \mathrm{lt}(\lambda_i f_i) + \xi_i$, i.e. $c_i \eta \cdot \mathrm{lt}(\lambda_i f_i) = \eta \cdot \lambda_i f_i - \xi_i$,

where $c_i = \mathrm{lc}(\eta \cdot \lambda_i f_i)$ and $\mathrm{lt}(\xi_i) \prec \eta \cdot \mathrm{lt}(\lambda_i f_i)$. Therefore

$$r = \frac{\mathrm{lc}(r)}{c_i}(\eta\lambda_i f_i - \xi_i) + \tilde{r} = \frac{\mathrm{lc}(r)}{c_i}\eta\lambda_i f_i + \underbrace{(\tilde{r} - \frac{\mathrm{lc}(r)}{c_i}\xi_i)}_{r'}.$$

Now we may replace r by r' and h_i by $h_i + \frac{\mathrm{lc}(r)}{c_i}\eta\lambda_i$. We continue this process as long as $r \ne 0$ and $\mathrm{lt}(r)$ is a multiple of some $\mathrm{lt}(\lambda_i f_i)$. Since in each step we have

$$\mathrm{lt}(r') \prec \mathrm{lt}(\eta \cdot \lambda_i f_i) \preceq \mathrm{lt}(r) \preceq \mathrm{lt}(g),$$

by the Corollary to Lemma 2.1, the algorithm above terminates after finitely many iterations. □

Observe that by Proposition 3.1 the statement in part (i) of Theorem 3.1 means that $\lambda u \preceq \mathrm{lt}(g)$ for all terms λ of h_i and all terms u of f_i. The r is by no means unique.

Definition 3.4. *Let $f_1, \ldots, f_p \in F \setminus \{0\}$, $g \in F$. Suppose that equation (3.2) holds and the conditions (i), (ii) in Theorem 3.1 are satisfied. If $r \neq g$ we say g can be* reduced *by $\{f_1, \cdots, f_p\}$ to r. In this case we have $\mathrm{lt}(r) \prec \mathrm{lt}(g)$ by the proof of Theorem 3.1. In the case of $r = g$ and $h_i = 0$ for $i = 1, \cdots, p$, we say that g* is reduced *w.r.t. $\{f_1, \cdots, f_p\}$.*

The following example illustrates the reason for Condition (ii) in Theorem 3.1.

Example 3.1. *Let $K = \mathbb{Q}(x_1, x_2)$, $D = K[\delta_1, \delta_2, \alpha, \alpha^{-1}]$, where δ_1, δ_2 are the partial derivatives w.r.t. x_1, x_2, respectively, and α is an automorphism of K. So D is the $\{\delta_1, \delta_2\}$–$\{\alpha\}$-ring over the coefficient field $\mathbb{Q}(x_1, x_2)$. Choose the generalized term order on $\mathbb{N}^2 \times \mathbb{Z}$ as in Example 2.3 (a), i.e.*

$$u = \delta_1^{k_1}\delta_2^{k_2}\alpha^l \prec v = \delta_1^{r_1}\delta_2^{r_2}\alpha^s \iff (\|u\|, k_1, k_2, l) <_{lex} (\|v\|, r_1, r_2, s),$$

where $\|u\| = k_1 + k_2 + |l|$. Let

$$g = \delta_1\alpha^{-2} + \delta_2\alpha^2, \quad f = \delta_1\alpha^{-1} + \alpha.$$

Then

$$g = \delta_1\alpha^{-2} + \delta_2\alpha^2 = \alpha^{-1}(\delta_1\alpha^{-1} + \alpha) + (\delta_2\alpha^2 - 1) = \alpha^{-1}f + r_1.$$

Although $\mathrm{lt}(r_1) = \delta_2\alpha^2$ is not any multiple of $\mathrm{lt}(f) = \delta_1\alpha^{-1}$, we can find $\lambda = \delta_2\alpha$ such that $\mathrm{lt}(r_1) = \mathrm{lt}(\lambda f) = \mathrm{lt}(\delta_1\delta_2 + \delta_2\alpha^2)$. Therefore

$$g = \alpha^{-1}f + \delta_2\alpha f + (-\delta_1\delta_2 - 1) = (\alpha^{-1} + \delta_2\alpha)f + r_2$$

Now r_2 satisfies the condition (ii) in Theorem 3.1. So g is reduced by f to r_2.

Definition 3.5. *Let W be a submodule of the finitely generated free D-module F and $\prec$ be a generalized term order on ΛE. Let $G = \{g_1, \cdots, g_p\} \subseteq W \setminus \{0\}$. Then G is called a* Gröbner basis *of W (w.r.t. the generalized term order $\prec$) if and only if for every $f \in W \setminus \{0\}$, $\mathrm{lt}(f)$ is a multiple of $\mathrm{lt}(\lambda g_j)$ for some $\lambda \in \Lambda$, $g_j \in G$. If every element of G is reduced with respect to the other elements of G, then G is called a* reduced Gröbner basis *of W.*

Proposition 3.2. *Let G be a finite subset of $W \setminus \{0\}$. The following assertions hold:*

(i) G is a Gröbner basis of W if and only if every $f \in W$ can be reduced by G to 0. So a Gröbner basis of W generates the D-module W.

(ii) If G is a Gröbner basis of W, $f \in F$, then $f \in W$ if and only if f can be reduced by G to 0.

(iii) If G is a Gröbner basis of W, then $f \in W$ is reduced w.r.t. G if and only if $f = 0$.

Proof. (i) If G is a Gröbner basis of W and $f \in W$, then by Theorem 3.1 f can be reduced by G to r with $\mathrm{lt}(r)$ not being a multiple of any $\mathrm{lt}(\lambda g)$ for $\lambda \in \Lambda, g \in G$. Since $r \in W$ and G is a Gröbner basis for W, we must have $r = 0$.

On the other hand, if every $f \in W$ can be reduced by G to 0, then $f = \sum_{g \in G} h_g g$. By Proposition 3.1, there is a $g \in G$ such that $\mathrm{lt}(f) = \max_{g \in G}\{\mathrm{lt}(h_g g)\} = \lambda u$ for a term of h_g and a term of g. So $\mathrm{lt}(f) = \mathrm{lt}(\lambda g)$. By Definition 3.5 G is a Gröbner basis of W.

(ii) and (iii) follow easily from Theorem 3.1 and Definition 3.5. □

Example 3.2. *If W is generated by just one element $g \in F \setminus \{0\}$, then any finite subset G of $W \setminus \{0\}$ containing g is a Gröbner basis of W. In fact, $0 \neq f \in W$ implies $f = hg$ for some $h \in D \setminus \{0\}$. By Proposition 3.1, $\mathrm{lt}(f) = \lambda u = \max_{\prec}\{\lambda_i u_k\}$ for a term λ of h and a term u of g. Then $\mathrm{lt}(f) = \mathrm{lt}(\lambda g)$. By Definition 3.5, G is a Gröbner basis of W.*

Now we will describe the Buchberger algorithm for computing a Gröbner basis of a submodule W of F. This requires a suitable definition of the concept of S-polynomial.

Definition 3.6. *Let F be a finitely generated free D-module and $f, g \in F \setminus \{0\}$. For every Λ_j let $V(j, f, g)$ be a finite system of generators of the $K[\Lambda_j]$-module*

$$_{K[\Lambda_j]}\langle \mathrm{lt}(\lambda f) | \mathrm{lt}(\lambda f) \in \Lambda_j E, \lambda \in \Lambda\rangle \cap {}_{K[\Lambda_j]}\langle \mathrm{lt}(\eta g) | \mathrm{lt}(\eta g) \in \Lambda_j E, \eta \in \Lambda\rangle.$$

Then for every generator $v \in V(j, f, g)$,

$$S(j, f, g, v) = \frac{v}{lt_j(f)}\frac{f}{lc_j(f)} - \frac{v}{lt_j(g)}\frac{g}{lc_j(g)}$$

is called an S-polynomial *of f and g with respect to j and v.*

The $K[\Lambda_j]$-module considered in Definition 3.6 is a "monomial module", i.e. it is generated by elements containing only one term. Such a module always has a finite "monomial basis", i.e. every basis element contains only one term. In the following we assume that $V(j, f, g)$ is such a finite monomial basis.

The computation of $V(j, f, g)$ involves the generalized term order on ΛE. Pauer and Unterkircher [12] have investigated $V(j, f, g)$ for commutative Laurent polynomial rings and have given algorithms for some important cases. Their results are still valid for difference-differential modules.

Example 3.3. *Let $F = D = K[\delta_1, \delta_2, \alpha_1, \alpha_1^{-1}, \alpha_2, \alpha_2^{-1}]$ and $K = \mathbb{Q}(x_1, x_2)$, where δ_1, δ_2 are the partial derivatives w.r.t. x_1 and x_2, respectively, and α_1, α_2 are two automorphism on K. Choose the generalized term order on $\mathbb{N}^2 \times \mathbb{Z}^2$ as in Example 2.3(c), i.e.*

$$u = \delta_1^{k_1}\delta_2^{k_2}\alpha_1^{l_1}\alpha_2^{l_2} \prec v = \delta_1^{r_1}\delta_2^{r_2}\alpha_1^{s_1}\alpha_2^{s_2}$$

$$\iff (\|u\|, k_1, k_2, l_1, l_2) \ <_{lex} \ (\|v\|, r_1, r_2, s_1, s_2),$$

where $\|u\| = -min(0, l_1, l_2)$.

Let $f = \alpha_1^{-2} - \delta_2$, $g = \delta_1 + \alpha_2^4$. Note that the orthants of Λ are $\Lambda_0, \Lambda_1, \Lambda_2$ as described in Example 2.2 for $n = 2$. It is easy to see that

$$\{\lambda \in \Lambda \mid \mathrm{lt}(\lambda f) \in \Lambda_0\} = \Lambda_0\alpha_1^2\ , \ \{\eta \in \Lambda \mid \mathrm{lt}(\eta g) \in \Lambda_0\} = \Lambda_0$$

and

$$\{\mathrm{lt}(\lambda f) \in \Lambda_0 \mid \lambda \in \Lambda\} = \Lambda_0\delta_2\alpha_1^2,$$
$$\{\mathrm{lt}(\eta g) \in \Lambda_0 \mid \eta \in \Lambda\} = \Lambda_0\delta_1.$$

Then $V(0,f,g)=\{v_0\}=\{\delta_1\delta_2\alpha_1^2\}$ *and by Definition 3.6,*

$$S(0,f,g,v_0)=\delta_1\alpha_1^2 f+\delta_2\alpha_1^2 g=\delta_1+\delta_2\alpha_1^2\alpha_2^4.$$

Similarly we have

$$\{\lambda\in\Lambda\mid \mathrm{lt}(\lambda f)\in\Lambda_1\}=\Lambda_1\alpha_1\ ,\ \{\eta\in\Lambda\mid \mathrm{lt}(\eta g)\in\Lambda_1\}=\Lambda_1$$

and

$$\begin{aligned}\{\mathrm{lt}(\lambda f)\in\Lambda_1\mid\lambda\in\Lambda\}&=\Lambda_1\alpha_1^{-1},\\ \{\mathrm{lt}(\eta g)\in\Lambda_1\mid\eta\in\Lambda\}&=\Lambda_1\delta_1.\end{aligned}$$

Then $V(1,f,g)=\{v_1\}=\{\delta_1\alpha_1^{-1}\}$ *and*

$$S(1,f,g,v_1)=\delta_1\alpha_1 f-\alpha_1^{-1}g=-\delta_1\delta_2\alpha_1-\alpha_1^{-1}\alpha_2^4.$$

Finally,

$$\begin{aligned}\{\lambda\in\Lambda\mid \mathrm{lt}(\lambda f)\in\Lambda_2\}&=\Lambda_2\alpha_1^2,\\ \{\eta\in\Lambda\mid \mathrm{lt}(\eta g)\in\Lambda_2\}&=\Lambda_2\alpha_2^{-1},\\ \{\mathrm{lt}(\lambda f)\in\Lambda_2\mid\lambda\in\Lambda\}&=\Lambda_2\delta_2\alpha_1^2,\\ \{\mathrm{lt}(\eta g)\in\Lambda_2\mid\eta\in\Lambda\}&=\Lambda_2\delta_1\alpha_2^{-1}.\end{aligned}$$

Then $V(2,f,g)=\{v_2\}=\{\delta_1\delta_2\alpha_1\alpha_2^{-1}\}$ *and*

$$S(2,f,g,v_2)=\delta_1\alpha_1\alpha_2^{-1}f+\delta_2\alpha_1\alpha_2^{-1}g=\delta_1\alpha_1^{-1}\alpha_2^{-2}+\delta_2\alpha_1\alpha_2^3.$$

For the proof of the Generalized Buchberger Theorem we need the following lemmas.

Lemma 3.4. *Let* $f_1,\cdots,f_l\in F$ *and* $a_1,\cdots,a_l\in K$. *If* $\sum_{j=1}^l a_j=0$, *then*

$$\sum_{j=1}^{l}a_jr_j=\sum_{j=1}^{l-1}b_j(f_j-f_{j+1})$$

for some $b_j\in R$.

Proof. Obviously

$\sum_{j=1}^l a_jr_j=$
$a_1(r_1-r_2)+(a_1+a_2)(r_2-r_3)+(a_1+a_2+a_3)(r_3-r_4)$
$+\cdots$
$+(a_1+a_2+\cdots+a_{l-1})(r_{l-1}-r_l)+(a_1+a_2+\cdots+a_l)r_l.$

□

Lemma 3.5. *Let* $g_i,\ g_k\in F$ *and* $lt(\lambda g_i)=lt(\eta g_k)=u\in\Lambda_jE$, *where* $\lambda,\ \eta\in\Lambda$. *Then there exists* $\zeta\in\Lambda_j$ *and* $v\in V(j,g_i,g_k)$, *such that* $u=\zeta v$. *Therefore if* G *is a finite subset of* $F\backslash\{0\}$ *and the S-polynomial* $S(j,g_i,g_k,v)$ *can be reduced to 0 by* G *then*

$$\zeta S(j,g_i,g_k,v)=\frac{u}{lt_j(g_i)}\frac{g_i}{lc_j(g_i)}-\frac{u}{lt_j(g_k)}\frac{g_k}{lc_j(g_k)}=\sum_{g\in G}h_gg$$

with $lt(h_gg)\prec u$ *for* $g\in G$.

Proof. Suppose $V(j,g_i,g_k)=\{v_1,\cdots,v_l\}$. Then

$$u=\sum_\mu p_\mu v_\mu,$$

where $p_\mu\in K[\Lambda_j]$. Since $p_\mu=\sum_\nu a_{\mu\nu}\lambda_{\mu\nu}$, where $a_{\mu\nu}\in K$ and $\lambda_{\mu\nu}\in\Lambda_j$, it follows that

$$u=\sum_{\mu,\nu}a_{\mu\nu}(\lambda_{\mu\nu}v_\mu). \qquad (*)$$

Note that u and $\lambda_{\mu\nu}v_\mu$ are terms in Λ_jE and we can rewrite the right hand side of the equation (*) such that the terms $\lambda_{\mu\nu}v_\mu$ are distinct. Then we see that there is a unique $a_{\mu\nu}=1$ and all others are zero. So $u=\zeta v$ for a $\zeta\in\Lambda_j$ and $v\in V(j,g_i,g_k)$.

Now if $S(j,g_i,g_k,v)$ can be reduced to 0 by G then

$$S(j,g_i,g_k,v)=\sum_{g\in G}h'_gg$$

and $\mathrm{lt}(h'_gg)\preceq\mathrm{lt}(S(j,g_i,g_k,v))\prec v$ for $g\in G$. Therefore

$$\zeta S(j,g_i,g_k,v)=\sum_{g\in G}(\zeta h'_g)g=\sum_{g\in G}h_gg,$$

where $h_g=\zeta h'_g$. By Lemma 3.2 (i), $\mathrm{lt}(\zeta h'_gg)=\zeta w$ for a term w of h'_gg. Then $\mathrm{lt}(h_gg)=\mathrm{lt}(\zeta h'_gg)=\zeta w$. Therefore $w\preceq\mathrm{lt}(h'_gg)\prec v$ and $\zeta\in\Lambda_j$ imply that $\zeta w\prec\zeta v=u$. □

Theorem 3.2. *(Generalized Buchberger Theorem) Let* F *be a free* D*-module and* $\prec$ *be a generalized term order on* ΛE, G *be a finite subset of* $F\backslash\{0\}$ *and* W *be the submodule in* F *generated by* G. *Then* G *is a Gröbner basis of* W *if and only if for all* Λ_j, *for all* $g_i,\ g_k\in G$ *and for all* $v\in V(j,g_i,g_k)$, *the S-polynomials* $S(j,g_i,g_k,v)$ *can be reduced to 0 by* G.

Proof. If G is a Gröbner basis of W, since $S(j,g_i,g_k,v)$ is a element of W, then it follows from Proposition 3.2 that $S(j,g_i,g_k,v)$ can be reduced to 0 by G.

Now let G be a finite subset of $F\backslash\{0\}$ and W be the submodule in F generated by G. Suppose that for all Λ_j, for all $g_i,\ g_k\in G$, and for all $v\in V(j,g_i,g_k)$ the S-polynomials $S(j,g_i,g_k,v)$ can be reduced to 0 by G. We have to show for every $f\in W\backslash\{0\}$ there are $\lambda\in\Lambda,\ g\in G$ such that $\mathrm{lt}(f)=\mathrm{lt}(\lambda g)$. Since W is generated by G, we have

$$f=\sum_{g\in G}h_gg$$

for some $\{h_g\}_{g\in G}\subseteq D$.

Let $u=\max_\prec\{\mathrm{lt}(h_gg)\mid g\in G\}$. We may choose the family $\{h_g\mid g\in G\}$ such that u is minimal, i.e. if $f=\sum_{g\in G}h'_gg$ then $u\preceq max_\prec\{\mathrm{lt}(h'_gg)\mid g\in G\}$. Note that $u\succeq\lambda g$ for all terms λ of h_g and all $g\in G$ by Proposition 3.1.

If $\mathrm{lt}(f)=u=\mathrm{lt}(h_gg)$ for some $g\in G$, then Proposition 3.1 implies that there is a term λ of h_g such that $\mathrm{lt}(f)=\mathrm{lt}(\lambda g)$. Therefore the proof would be completed. Hence it remains to show that $\mathrm{lt}(f)\prec u$ cannot hold.

Suppose $\mathrm{lt}(f)\prec u$ and let $B=\{g\mid\mathrm{lt}(h_gg)=u\succ\mathrm{lt}(f)\}$. Then, by Proposition 3.1, there is a unique term λ_g of h_g, $g\in B$, such that $u=\mathrm{lt}(\lambda_gg)\succ\mathrm{lt}(\eta_gg)$ for any terms $\eta_g\neq\lambda_g$ of h_g. Let c_g be the coefficient of λ_g in h_g. We have

$$\begin{aligned}f&=\textstyle\sum_{g\in B}h_gg+\sum_{g\notin B}h_gg\\ &=\textstyle\sum_{g\in B}c_g\lambda_gg+\sum_{g\in B}(h_g-c_g\lambda_g)g+\sum_{g\notin B}h_gg,\end{aligned}\qquad(3.3)$$

where all terms appearing in the last two sums are less than u w.r.t. $\prec$.

Suppose v_g is the term of g such that $u=\mathrm{lt}(\lambda_gg)=\lambda_gv_g\succ\lambda_gv$ for any terms $v\neq v_g$ of g, according to Lemma 3.2(i). Let d_g be the coefficient of v_g in g. Then by Lemma 3.1,

$$\begin{aligned}\textstyle\sum_{g\in B}c_g\lambda_g&=\textstyle\sum_{g\in B}c_g\lambda_gd_g(\frac{g}{d_g})\\ &=\textstyle\sum_{g\in B}c_g(d'_g\lambda_g+\xi_g)(\frac{g}{d_g})\\ &=\textstyle\sum_{g\in B}c_gd'_g\lambda_g(\frac{g}{d_g})+\sum_{g\in B}c_g\xi_g(\frac{g}{d_g})\end{aligned}\qquad(3.4)$$

for some elements $d'_g \in K$ and $\xi_g \in D$ with all terms appearing in the last sum being less than u w.r.t. $\prec$.

Note that u appears only in

$$\begin{array}{l}\sum_{g\in B} c_g d'_g \lambda_g(\frac{g}{d_g}) = \\ \sum_{g\in B} c_g d'_g \lambda_g v_g + \sum_{g\in B} c_g d'_g \lambda_g(\frac{g}{d_g} - v_g) = \\ (\sum_{g\in B} c_g d'_g)u + \sum_{g\in B} c_g d'_g \lambda_g(\frac{g}{d_g} - v_g)\end{array}$$

and all terms appearing in the last sum are less than u. Since $\mathrm{lt}(f) \prec u$ it follows that $\sum_{g\in B} c_g d'_g = 0$. Denote $\lambda_g(\frac{g}{d_g})$ by r_g. Then by Lemma 3.4,

$$\sum_{g\in B} c_g d'_g \lambda_g(\frac{g}{d_g}) = \sum_{g\in B}(c_g d'_g) r_g = \sum_{i,k} b_{i,k}(r_{g_i} - r_{g_k}) \quad (3.5)$$

for some $g_i,\ g_k \in B$.

Since

$$r_{g_i} - r_{g_k} = \lambda_{g_i}(\frac{g_i}{d_{g_i}}) - \lambda_{g_k}(\frac{g_k}{d_{g_k}})$$

and $\lambda_{g_i} v_{g_i} = \lambda_{g_k} v_{g_k} = u \in \Lambda_j E$ for an Λ_j, it follows from Lemma 3.3 that $v_{g_i} = lt_j(g_i)$, $v_{g_k} = lt_j(g_k)$, $d_{g_i} = lc_j(g_i)$, $d_{g_k} = lc_j(g_k)$, $\lambda_{g_i} = \frac{u}{lt_j(g_i)}$, $\lambda_{g_k} = \frac{u}{lt_j(g_k)}$ and then

$$r_{g_i} - r_{g_k} = \frac{u}{lt_j(g_i)}\frac{g_i}{lc_j(g_i)} - \frac{u}{lt_k(g_k)}\frac{g_k}{lc_j(g_k)}$$

with $lt(r_{g_i} - r_{g_k}) \prec u$.

Note that for all Λ_j, for all $g_i,\ g_k \in G$, and for all $v \in V(j, g_i, g_k)$ the S-polynomials $S(j, g_i, g_k, v)$ can be reduced to 0 by G. Then by Lemma 3.5, we have

$$r_{g_i} - r_{g_k} = \sum_{g\in G} p_g g \quad (3.6)$$

with $lt(p_g g) \prec u$.

Replace the first sum in the r.h.s. of (3.3) by (3.4), and replace the first sum in the r.h.s. of (3.4) by (3.5), then replace $r_{g_i} - r_{g_k}$ in the r.h.s. of (3.5) by (3.6). We get another form of $f = \sum_{g\in G} h'_g g$ and $u \succ \max_{\prec}\{\mathrm{lt}(h'_g g) \mid g \in G\}$, which is a contradiction to the minimality of u. This completes the proof of the theorem. □

Example 3.4. *If W is a submodule of F generated by a finite set G and every $g \in G$ consists of only one term, then G is a Gröbner basis of W. In fact in this case all S-polynomials $S(j, g_i, g_k, v)$ are 0. By Theorem 3.2 this implies that G is a Gröbner basis of W.*

Theorem 3.3. *(Buchberger Algorithm) Let F be a free D-module and $\prec$ be a generalized term order on ΛE, G be a finite subset of $F\backslash\{0\}$ and W be the submodule in F generated by G. For each Λ_j and $f, g \in F\backslash\{0\}$ let $V(j, f, g)$ and $S(j, f, g, v)$ be as in Definition 3.6. Then by the following algorithm a Gröbner basis of W can be computed:*

Input: $G = \{g_1, \cdots, g_\mu\}$ *which is a set of generators of* W
Output: $G' = \{g'_1, \cdots, g'_\nu\}$ *which is a Gröbner basis of* W
Begin
  $G_0 := G$
  While *there exist* $f, g \in G_i$ *and* $v \in V(j, f, g)$ *such that* $S(j, f, g, v)$ *reduces to* $r \neq 0$ *by* G_i
  Do $G_{i+1} := G_i \cup \{r\}$
  If $G_{i+1} = G_i$ **then** $G_{i+1} = G'$
End

Proof. By Theorem 3.2 we only have to show that there is an $i \in \mathbb{N}$ such that $G_{i+1} = G_i$. Suppose there is no such $i \in \mathbb{N}$. In every step of the algorithm we get an r such that $\mathrm{lt}(r)$ is not a multiple of any $\mathrm{lt}(\lambda g)$, where $\lambda \in \Lambda$ and $g \in G_i$. So if $\mathrm{lt}(r) \in \Lambda_j E$ then

$$\begin{array}{rcl} K_j^{(i)} & = & {}_{K[\Lambda_j]}\langle \mathrm{lt}(\lambda g) \in \Lambda_j E \mid \lambda \in \Lambda,\ g \in G_i\rangle \\ & \subsetneq & {}_{K[\Lambda_j]}\langle \mathrm{lt}(\lambda g) \in \Lambda_j E \mid \lambda \in \Lambda,\ g \in G_{i+1}\rangle \\ & = & K_j^{(i+1)} \end{array}$$

as $K[\Lambda_j]$-submodules of $\bigoplus_{e\in E} K[\Lambda_j]e$. Therefore, for all $i \in \mathbb{N}$ there is an $m \in \mathbb{N}$ such that

$$K_j^{(i)} \subsetneq K_j^{(i+m)}.$$

This, however, is impossible because of the Noetherianity of $K[\Lambda_j]$. □

Example 3.5. *Let F and the generalized term order on Λ be as in Example 3.3. Let $G = \{g_1, g_2, g_3\} = \{\alpha_2^4 + 1, \alpha_1^2 - 1, \alpha_1^2\alpha_2^4 + 1\}$. Then G is a Gröbner basis of the submodule W generated by G. To prove this, we must show that all S-polynomials of G can be reduced to 0 by G.*

Following the method described in Example 3.3, we have $V(0, g_1, g_2) = \{\alpha_1^2\alpha_2^4\}$, $V(1, g_1, g_2) = \{\alpha_1^{-1}\alpha_2^3\}$, $V(2, g_1, g_2) = \{\alpha_1\alpha_2^{-1}\}$. So

$$\begin{array}{rcl} S(0, g_1, g_2, \alpha_1^2\alpha_2^4) & = & \alpha_1^2 g_1 - \alpha_2^4 g_2 = \alpha_1^2 + \alpha_2^4 = g_1 + g_2, \\ S(1, g_1, g_2, \alpha_1^{-1}\alpha_2^3) & = & \alpha_1^{-1}\alpha_2^{-1} g_1 + \alpha_1^{-1}\alpha_2^3 g_2 = \\ & & \alpha_1^{-1}\alpha_2^{-1} + \alpha_1\alpha_2^3 = (\alpha_1^{-1}\alpha_2^{-1})g_3, \\ S(2, g_1, g_2, \alpha_1\alpha_2^{-1}) & = & \alpha_1\alpha_2^{-1} g_1 - \alpha_1^{-1}\alpha_2^{-1} g_2 = \\ & & \alpha_1^{-1}\alpha_2^{-1} + \alpha_1\alpha_2^3 = (\alpha_1^{-1}\alpha_2^{-1})g_3. \end{array}$$

Furthermore, $V(0, g_1, g_3) = \{\alpha_1^2\alpha_2^4\}$, $V(1, g_1, g_3) = \{\alpha_1^{-1}\alpha_2^3\}$, $V(2, g_1, g_3) = \{\alpha_2^{-1}\}$. So

$$\begin{array}{rcl} S(0, g_1, g_3, \alpha_1^2\alpha_2^4) & = & \alpha_1^2 g_1 - g_3 = \alpha_1^2 - 1 = g_2, \\ S(1, g_1, g_3, \alpha_1^{-1}\alpha_2^3) & = & \alpha_1^{-1}\alpha_2^{-1} g_1 - \alpha_1^{-1}\alpha_2^3 g_3 = \\ & & \alpha_1^{-1}\alpha_2^{-1} - \alpha_1\alpha_2^7 = \\ & & (\alpha_1^{-1}\alpha_2^{-1})g_3 - \alpha_1\alpha_2^3 g_1, \end{array}$$

(note that the r.h.s. of this equation satisfies the condition in Theorem 3.1 (i), i.e. $\mathrm{lt}(h_i g_i) \preceq \mathrm{lt}(S)$*)*

$$S(2, g_1, g_3, \alpha_2^{-1}) = \alpha_2^{-1} g_1 - \alpha_2^{-1} g_3 = \alpha_2^3 - \alpha_1^2\alpha_2^3 = -\alpha_2^3 g_2.$$

Finally, $V(0, g_2, g_3) = \{\alpha_1^2\alpha_2^4\}$, $V(1, g_2, g_3) = \{\alpha_1^{-1}\}$, $V(2, g_2, g_3) = \{\alpha_1\alpha_2^{-1}\}$. So

$$\begin{array}{rcl} S(0, g_2, g_3, \alpha_1^2\alpha_2^4) & = & \alpha_2^4 g_2 - g_3 = -\alpha_2^4 - 1 = -g_1, \\ S(1, g_2, g_3, \alpha_1^{-1}) & = & \alpha_1^{-1} g_2 - \alpha_1^{-1} g_3 = \alpha_1\alpha_2^4 + \alpha_1 = \\ & & \alpha_1 g_1, \\ S(2, g_2, g_3, \alpha_1\alpha_2^{-1}) & = & \alpha_1^{-1}\alpha_2^{-1} g_2 - \alpha_1\alpha_2^{-1} g_3 = \\ & & -\alpha_1^{-1}\alpha_2^{-1} - \alpha_1^3\alpha_2^3 = \\ & & \alpha_1^{-1}\alpha_2^{-1} g_3 + \alpha_1\alpha_2^3 g_2. \end{array}$$

The r.h.s. of this equation also satisfies the condition in Theorem 3.1 (i). So, by Theorem 3.2, G is a Gröbner basis of W.

4. ACKNOWLEDGMENTS

This work has been supported by the Austrian FWF project P16357-N04 and by the National Key Basic Research Project 2005CB321902 of China, while the first author spent a research year at RISC-Linz.

5. REFERENCES

[1] T. Becker, V. Weispfenning. *Gröbner bases. A Computational Approach to Commutative Algebra.* Spinger-Verlag, New York (1993).

[2] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph.D. dissertation, Univ. Innsbruck, Austria (1965).

[3] B. Buchberger. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *J. Symb. Comp.* 41/3-4, 475–511 (2006).

[4] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms,* 2nd ed. Springer-Verlag, New York (1997)

[5] A. Galligo. Some algorithmic questions on ideals of differential operators. *Proc. EUROCAL'85*, B.F. Caviness (ed.), LNCS 204, 413-421, Springer-Verlag, Berlin (1985).

[6] M. Insa, F. Pauer. Gröbner bases in rings of differential operators. In *Gröbner Bases and Applications*, B. Buchberger and F. Winkler (eds.), 367-380, Cambridge University Press (1998).

[7] M.V. Kondrateva, A.B. Levin, A.V. Mikhalev and E.V. Pankratev. *Differential and Difference Dimension Polynomials.* Kluwer Acad. Publ., Dordrecht (1998).

[8] A.B. Levin. Reduced Gröbner bases, free difference-differential modules and difference-differential dimension polynomials. *J. Symb. Comput.* 30/4, 357-382 (2000).

[9] T. Mora. Gröbner bases for non-commutative polynomial rings. In *Proc. AAECC-3*, J. Calmet (ed.), LNCS 229, 353-362, Springer-Verlag (1986).

[10] M. Noumi. Wronskian determinants and the Gröbner representation of linear differential equations. In *Algebraic Analysis*, M. Kashiwara, T. Kawai (eds.), 549-569, Academic Press, Boston (1988).

[11] T. Oaku, T. Shimoyama. A Gröbner basis method for modules over rings of differential operators. *J. Symb. Comput.* 18/3, 223-248 (1994).

[12] F. Pauer, A. Unterkircher. Gröbner bases for ideals in Laurent polynomial rings and their applications to systems of difference equations. *AAECC* 9, 271-291 (1999).

[13] N. Takayama. Gröbner basis and the problem of contiguous relations. *Japan J. Appl. Math.* 6, 147-160 (1989).

[14] F. Winkler. *Polynomial Algorithms in Computer Algebra.* Springer-Verlag, Wien New York (1996).

[15] M. Zhou, F. Winkler. Gröbner bases in difference-differential modules and their applications. Techn.Rep. 05-14, RISC, J.Kepler Univ. Linz, Austria (2005).