.

SKEW POLYNOMIAL RINGS, GRÖBNER BASES AND THE LETTERPLACE EMBEDDING OF THE FREE ASSOCIATIVE ALGEBRA

ROBERTO LA SCALA* AND VIKTOR LEVANDOVSKYY**

Abstract. In this paper we introduce an algebra embedding $\iota : K\langle X\rangle \to S$ from the free associative algebra $K\langle X\rangle$ generated by a finite or countable set X into the skew monoid ring $S = P * \Sigma$ defined by the commutative polynomial ring $P = K[X \times \mathbb{N}^*]$ and by the monoid $\Sigma = \langle\sigma\rangle$ generated by a suitable endomorphism $\sigma : P \to P$. If $P = K[X]$ is any ring of polynomials in a countable set of commuting variables, we present also a general Gröbner bases theory for graded two-sided ideals of the graded algebra $S = \bigoplus_i S_i$ with $S_i = P\sigma^i$ and $\sigma : P \to P$ an abstract endomorphism satisfying compatibility conditions with ordering and divisibility of the monomials of P. Moreover, using a suitable $\mathbb{N}$-grading for the algebra P compatible with the action of Σ, we obtain a bijective correspondence, preserving Gröbner bases, between graded Σ-invariant ideals of P and a class of graded two-sided ideals of S. By means of the embedding ι this results in the unification, in the graded case, of the Gröbner bases theories for commutative and non-commutative polynomial rings. Finally, since the shift operators $x_i \mapsto x_{i+1}$ fits the proposed theory for $X = \{x_1, x_2, \ldots\}$, one obtains also that Gröbner bases of finitely generated graded ordinary difference ideals can be computed by these methods in the operators ring S and in a finite number of steps up to some degree.

1. Introduction

Let P be a K-algebra and let Σ be a monoid of endomorphisms of P. If I is an ideal of P which is invariant under the maps in Σ then it is possible to codify the action of P and Σ over I as a single left module structure with respect to the skew monoid (or semigroup) ring $S = P * \Sigma$. The study of some properties of I, as for instance its finite Σ-generation, can be reduced hence to that of general properties of the operators ring S as its Noetherianity (see [20, 16]). Ideals which are stable under the action of monoids of endomorphisms or groups of automorphisms are natural in many contexts as the representation theory (a classical reference is [5]), or in the study of PI-algebras [7, 11] where P is the free associative algebra and Σ the complete monoid of endomorphisms of P. Another context of relevant interest is the study of so-called "difference ideals" [18] which are ideals invariant under shift operators in applications to combinatorics, (nonlinear) differential and difference equations.

To control in an effective way the structure of the left S-module P/I one generally needs to compute a K-basis of it. If P is a ring of polynomials in commutive or non-commutative variables and one fixes a suitable ordering for the monomials of P,

2000 *Mathematics Subject Classification.* Primary 16Z05. Secondary 13P10, 68W30.

Key words and phrases. Skew polynomial rings; Free algebras; Gröbner bases.

Partially supported by Università di Bari, Ministero dell'Università e della Ricerca, and by the DFG Graduiertenkolleg "Hierarchie und Symmetrie in mathematischen Modellen" at RWTH Aachen, Germany.

then a K-linear basis of monomials for P/I can be obtained by using the elements of a suitable generating set of I as rewriting rules. Such generating set is usually called a "Gröbner basis" of I. Since I is a Σ-invariant ideal, it is natural to consider Σ-bases of I that is sets $G \subset I$ such that I is the smallest Σ-ideal of P containing G. In other words, G is a generating set of I as left S-module. It follows that one has to harmonize the notion of Gröbner basis with that of Σ-basis and attempts in this direction can be found for instance in [1, 3] and also in [8, 17]. If the elements of Σ are automorphisms, the main obstacle in the definition of a Gröbner Σ-basis is that their action on P does not preserve the monomial ordering. Then, it has been shown in [3] and before in [17] that an appropriate setting to define Gröbner Σ-bases is that of a commutative polynomial ring $P = K[X]$ in an infinite number of variables and a monoid Σ of monomial monomorphisms of infinite order which are compatible with the ordering and divisibility of monomials of P.

In this paper we propose a systematic study of the case when Σ is generated by a single map σ. In this case the skew monoid ring S coincides with the skew polynomial ring $P[s;\sigma]$ which is an instance of Ore extension. The approach we follow is to consider an abstract map σ satisfying compatibility conditions able to provide a "natural" Gröbner bases theory. Note that this generalizes in particular the results contained in [23] where the map $\sigma : x_i \mapsto x_i^e$ with $e > 1$ has been studied. We choose to consider a single endomorphism essentially because a major application of our theory is the unification, in the graded case, of the Gröbner bases theory for non-commutative polynomials introduced in [12, 21, 22] with the classical commutative theory based on the notion of S-polynomial (see for instance [14]). In Section 6 we show in fact that there exists an algebra embedding $\iota : K\langle X\rangle \to S$ where $K\langle X\rangle$ is the free associative algebra generated by the variables x_i and S is the skew polynomial ring defined by the algebra P of commutative polynomials in double indexed variables $x_i(j)$ and the endomorphism $\sigma : P \to P$ such that $x_i(j) \mapsto x_i(j+1)$, for all i, j. This algebra embedding is a decisive improvement of the linear map $\iota' : K\langle X\rangle \to P$ defined as $x_{i_1}\cdots x_{i_d} \mapsto x_{i_1}(1)\cdots x_{i_d}(d)$ and introduced by [10, 6] for the aims of physics and invariant/representation theory. In fact, the use of the map ι clarify the phenomenon found in [17] of a bijective correspondence between all graded two-sided ideals of $K\langle X\rangle$ and some class of Σ-invariant ideals of P. Note that in the same paper, a competitive new algorithm for non-commutative homogeneous Gröbner bases based on this correspondence has been implemented and experimented in SINGULAR [4].

In Section 2 one finds a brief account of the general equivalence between the notion of Σ-invariant P-module and that of left S-module, together with the description of some properties of the generating sets of graded two-sided ideals of $S = \bigoplus_i S_i$ with $S_i = Ps^i$. A Gröbner basis theory for such ideals is introduced in Section 3 where we assume $P = K[x_1, x_2, \ldots], \Sigma = \langle\sigma\rangle$ and $\sigma : P \to P$ be a monomorphism of infinite order sending monomials into monomials. Additional assuptions for σ are that $\gcd(\sigma(x_i), \sigma(x_j)) = 1$ for $i \neq j$ and the monomial ordering of P is such that $m \prec n$ implies that $\sigma(m) \prec \sigma(n)$, for all monomials m, n. Such conditions are quite natural in many contexts as the shift operators $x_i \mapsto x_{i+1}$ defining difference ideals [18] or the maps used in [3]. Note that the algorithms we introduce for the computation of homogeneous Gröbner bases in S are based on the free P-module structure of this ring and hence they appear as a variant of the classical module Buchberger algorithm where the number of S-polynomials to be considered is reduced owing to the symmetry defined by Σ on the graded ideals of the ring S.

In Section 5 we analyze the notion of Gröbner Σ-basis for Σ-invariant ideals of P. When P can be endowed with a suitable grading compatible with the action of Σ, we describe a bijective correspondence between all graded Σ-invariant ideals of P and some class of graded two-sided ideals of S. Such correspondence preserves Gröbner bases and gives rise to a duality between homogeneous algorithms in P and in S. Note that for finitely generated ideals all these procedures admit termination when truncated at some degree. As we said earlier, in Section 6 the algebra embedding $\iota : K\langle X\rangle \to S$ is introduced and a bijective correspondence between the ideals of $K\langle X\rangle$ and suitable ideals of S is hence obtained by extension. The Gröbner bases are preserved by this correspondence and one obtains an alternative algorithm for computing non-commutative homogeneous Gröbner bases of $K\langle X\rangle$ in the free P-module S. By means of the bijection of the Section 5, we reobtain in Section 7 the ideal correspondence and related algorithms introduced in [17] which provide the computation of non-commutative homogeneous Gröbner bases directly in P. Therefore, the theory for such bases can be deduced by the classical Buchberger algorithm for commutative polynomial rings. Finally in Chapter 8 we propose some conclusions and suggestions for future developments of the proposed theory and its methods.

2. Modules over skew monoid rings

Fix K any field and let P be a commutative K-algebra. Let now $\Sigma \subset \mathrm{End}_K(P)$ a submonoid of the monoid of K-algebra endomorphisms of P. Denote $S = P * \Sigma$ the *skew monoid ring defined by* Σ *over* P that is S is the free P-module with (left) basis Σ and the multiplication is defined by the identity $\sigma f = \sigma(f)\sigma$, for all $f \in P, \sigma \in \Sigma$. If $\Sigma \neq \{id\}$ then S is a non-commutative K-algebra where the ring P and the monoid Σ are embedded. Note that if $\Sigma = \langle\sigma\rangle$ with $\sigma : P \to P$ a map of infinite order one has that $S \approx P[s;\sigma]$, the skew polynomial ring in the variable s and coefficients in P defined by the endomorphism σ. Moreover, if P is a domain and all maps in Σ are injective then S is a also domain. To simplify notations, we denote $f^\sigma = \sigma(f)$ for any $f \in P, \sigma \in \Sigma$.

Definition 2.1. *Let M be a P-module. We call M* a Σ-invariant module *if there is a monoid homomorphism $\rho : \Sigma \to End_K(M)$ such that $\rho(\sigma)(fx) = f^\sigma \rho(\sigma)(x)$, for all $f \in P, x \in M$ and $\sigma \in \Sigma$. We denote as usual $\sigma \cdot x = \rho(\sigma)(x)$. If M, M' are Σ-invariant modules and $\varphi : M \to M'$ is a P-module homomorphism such that $\varphi(\sigma \cdot x) = \sigma \cdot \varphi(x)$ for all $x \in M, \sigma \in \Sigma$, then the map φ is called* a homomorphism of Σ-invariant modules.

Proposition 2.2. *The category of Σ-invariant P-modules is equal to the category of left S-modules.*

Proof. Let M be a left S-module. Then M is a P-module since $P \subset S$. By restriction to $\Sigma \subset S$, one has a monoid homomorphism $\rho : \Sigma \to \mathrm{End}_K(M)$. Moreover we have $\sigma \cdot (fx) = (\sigma f) \cdot x = (f^\sigma \sigma) \cdot x = f^\sigma(\sigma \cdot x)$, for all $f \in P, x \in M$ and $\sigma \in \Sigma$. Let now M be a Σ-invariant P-module. We can define a left S-module structure by putting $(\sum_i f_i\sigma_i) \cdot x = \sum_i f_i(\sigma_i \cdot x)$ with $f_i \in P, \sigma_i \in \Sigma$ and $x \in M$. Consider a homomorphism $\varphi : M \to M'$ of Σ-invariant modules. Since φ is P-linear, one has $\varphi((\sum_i f_i\sigma_i) \cdot x) = \sum_i f_i\varphi(\sigma_i \cdot x) = \sum_i f_i(\sigma_i \cdot \varphi(x)) = (\sum_i f_i\sigma_i) \cdot \varphi(x)$. $\square$

Let M be a left S-module and let $G = \{g_i\} \subset M$ be a generating set of M. Note that $x \in M$ if and only if $x = \sum_{i,\sigma} f_{i\sigma}\sigma \cdot g_i$ with $f_{i\sigma} \in P$ that is M is generated by $\Sigma \cdot G = \{\sigma \cdot g_i\}_{i,\sigma}$ as P-module. We want now to describe homogeneous bases for graded two-sided ideals of S. In fact, the algebra S has a natural grading over the monoid Σ that is $S = \bigoplus_{\sigma\in\Sigma} S_\sigma$ and $S_\sigma S_\tau \subset S_{\sigma\tau}$ where $S_\sigma = P\sigma$. Note that $S_{id} = P$, all S_σ are P-submodules of S and $S_\sigma \tau = S_{\sigma\tau}$.

Proposition 2.3. *Let $J \subset S$ be a graded (two-sided) ideal and let $G \subset J$ be a set of homogeneous elements. Then G is a generating set of J if and only if $G\,\Sigma$ is a left basis of J that is $\Sigma\, G\,\Sigma$ is a basis of J as P-module.*

Proof. Assume $G = \{g_i\sigma_i\}$ with $g_i \in P, \sigma_i \in \Sigma$, for all i. Let $p_i, q_i \in S$ with $q_i = \sum_\sigma q_{i\sigma}\sigma$ and $q_{i\sigma} \in P$. It is sufficient to note that $\sum_i p_i g_i \sigma^i q_i = \sum_{i,\sigma} p_i g_i \sigma^i q_{i\sigma}\sigma = \sum_{i,\sigma} p_i q_{i\sigma}^{\sigma_i} g_i \sigma_i \sigma$. ∎

Corollary 2.4. *Let $f, g \in S$ and let g be a homogeneous element. Then, one has that $f = pgq$ with $p, q \in S$ if and only if f belongs to the (graded) left ideal generated by $\{g\sigma\}_{\sigma\in\Sigma}$.*

3. Monomial orderings and Gröbner bases

From now on, $P = K[X]$ is the commutative polynomial ring generated by a countable set of variables $X = \{x_1, x_2, \ldots\}$. Moreover, we fix $\sigma : P \to P$ an algebra homomorphism of infinite order and define the monoid $\Sigma = \langle\sigma\rangle \approx \mathbb{N}$. Then, the skew monoid ring $S = P * \Sigma$ is isomorphic to the skew polynomial ring $P[s; \sigma]$ and we identify $\Sigma = \{\sigma^i\}$ with the monoid $\{s^i\}$ of powers of the variable s. Note that S is a free P-module of infinite rank. We denote $f^{s^i} = f^{\sigma^i} = \sigma^i(f)$, for all $f \in P, i \geq 0$. Moreover, a homogeneous element $f \in S_i = Ps^i$ for some i is also called *s-homogeneous* and we put $\deg_s(f) = i$. Note finally that in the theory of difference ideals [18], the ring S is called *ring of (ordinary) difference operators over* P.

Denote by $\mathrm{Mon}(P)$ the set of all monomials of P (including 1). Clearly, $\mathrm{Mon}(P)$ is a multiplicative K-basis of P that is $mn \in \mathrm{Mon}(P)$ for all $m, n \in \mathrm{Mon}(P)$. By definition of S, a K-basis of such algebra is given by the elements ms^i where $m \in \mathrm{Mon}(P)$ and $i \geq 0$ is an integer. We call such elements the *monomials of* S and we denote the set of them as $\mathrm{Mon}(S)$. Clearly $\mathrm{Mon}(P) \subset \mathrm{Mon}(S)$. Note that $\mathrm{Mon}(S)$ is in fact the "monomial basis" of S as a free P-module.

From now on, *we assume* that the endomorphism $\sigma : P \to P$ is injective and *monomial* that is it stabilizes the set $\mathrm{Mon}(P)$. In other words, $\{\sigma(x_i)\}$ is a set of algebraically independent monomials. Since P is a domain, it follows that S is also a domain and the K-basis $\mathrm{Mon}(S)$ is multiplicative since $ms^i ns^j = mn^{s_i}s^{i+j} \neq 0$, for all $m, n \in \mathrm{Mon}(P)$ and $i, j \geq 0$.

We want to study now some divisibility relations in $\mathrm{Mon}(S)$. Let $f, g \in S$. We say that f *left-divides* g if there is $a \in S$ such that $g = af$. Clearly, left divisibility is a partial ordering (up to units). Since σ is a monomial injective map, one has that if $f, g \in \mathrm{Mon}(S)$ then also $a \in \mathrm{Mon}(S)$.

Proposition 3.1. *Let $v = ms^i, w = ns^j \in \mathrm{Mon}(S)$ with $m, n \in \mathrm{Mon}(P)$. Then v left-divides w if and only if $i \leq j$ and $m^{s^{j-i}} \mid n$.*

Proof. Let $a = ps^k \in \mathrm{Mon}(S)$ with $p \in \mathrm{Mon}(P)$ such that $ns^j = ps^k ms^i = pm^{s^k}s^{k+i}$. Then, we have that $j - i = k \geq 0$ and $m^{s^k} \mid n$. ∎

Note that S has also a free P-module structure and so $\mathrm{Mon}(S)$ inherits another notion of divisibility. Precisely, let $v, w \in \mathrm{Mon}(S)$. We say that v *P-divides* w if $\deg_s(v) = \deg_s(w)$ and there is $a \in \mathrm{Mon}(P)$ such that $w = av$. Clearly P-divisibility is a partial ordering and one has the following result.

Proposition 3.2. *Let $v, w \in \mathrm{Mon}(S)$. Then v left-divides w if and only if $s^k v$ P-divides w for some $k \geq 0$.*

Note that left divisibility coincides with P-divisibility when the monomials have the same s-degree. If there are $v, w, a, b \in \mathrm{Mon}(S)$ such that $w = avb$ we say that v *(two-sided) divides* w. It is easy to prove that such divisibility is also a partial ordering.

Proposition 3.3. *Let $v, w \in \mathrm{Mon}(S)$. Then w is a multiple of v if and only if there is $j \geq 0$ such that w is a left multiple of vs^j, that is w is a P-multiple of $s^i v s^j$ for some $i, j \geq 0$.*

Proof. Since monomials are s-homogeneous elements of S, by applying Corollary 2.4 we obtain that w is a multiple of v if and only if w belongs to the (graded) left ideal generated by $\{vs^j\}_{j \geq 0}$. Clearly, this happens when w is a left multiple of vs^j for some j. □

We start now considering monomial orderings.

Definition 3.4. *Let $\prec$ be a total ordering on the set* $\mathrm{Mon}(S)$*. We call $\prec$ a* monomial ordering *of S if it satisfies the following conditions*

(i) *$\prec$ is a well-ordering, that is every non-empty set of* $\mathrm{Mon}(S)$ *has a minimal element;*
(ii) *$\prec$ is compatible with multiplication, that is if $v \prec w$ then $pvq \prec pwq$, for all $v, w, p, q \in \mathrm{Mon}(S)$.*

It follows immediately that $1 \preceq w$ for any $w \in \mathrm{Mon}(S)$ and if $w = pvq$ with $p \neq 1$ or $q \neq 1$ then $v \prec w$ for all $v, w, p, q \in \mathrm{Mon}(S)$. Note that the above conditions agree with general definitions of orderings on K-bases of associative algebras that provide a Gröbner basis theory (see for instance [13, 19]). The same conditions define monomial orderings of the free algebras $K\langle X \rangle$ and $K[X]$. Note that such algebras can be endowed with a monomial ordering even if the set of variables X is countable. This is provided by the Higman's lemma [15] which states that any multiplicatively compatible total ordering of the monomials such that $1 \prec x_1 \prec x_2 \prec \ldots$ is a monomial ordering. Recall that f^s stands for $\sigma(f)$ for any $f \in P$.

Definition 3.5. *Let $\prec$ be a monomial ordering on P. We call σ* compatible with *$\prec$ if σ is a strictly increasing map when restricted to* $\mathrm{Mon}(P)$*, that is $m \prec n$ implies that $m^s \prec n^s$ for all $m, n \in \mathrm{Mon}(P)$.*

The following result is based essentially on Remark 3.2 in [3].

Proposition 3.6. *Assume σ be compatible with $\prec$. Then σ is not an automorphism and $m \preceq m^s$, for all $m \in \mathrm{Mon}(P)$.*

Proof. Since $\sigma \neq id$, there is $m \in \mathrm{Mon}(S)$ such that $m \neq m^s$. If $m \succ m^s$, by compatibility of σ one gets an infinite descending chain $m \succ m^s \succ m^{s^2} \succ \ldots$ which contradicts the condition that $\prec$ is a well-ordering. We conclude that $m \prec m^s$.

Assume that σ has the inverse σ^{-1}. By applying σ, from $m^{s^{-1}} \prec n^{s^{-1}}$ it follows that $m \prec n$. Since σ^{-1} is injective, we have therefore that $m \prec n$ implies that $m^{s^{-1}} \prec n^{s^{-1}}$. Now, by compatibility of σ^{-1} we obtain $m \prec m^{s^{-1}}$ which contradicts $m \prec m^s$. $\square$

There are many endomorphisms σ with are compatible with usual monomial orderings on P like lex, degrevlex, etc. For instance, we have the following maps.

- $\sigma(x_i) = x_{f(i)}$ for any i, where $f : \mathbb{N}^* \to \mathbb{N}^*$ is a strictly increasing map. Such maps have been considered in [3]. In particular, one may define the shift operator $\sigma(x_i) = x_{i+1}$ which is used in difference algebra.
- $\sigma(x_i) = x_i^e$ for any i, with $e > 1$. This map has been considered in [23].

Proposition 3.7. *Let $\prec$ be a monomial ordering on S. Then σ is compatible with the restriction of $\prec$ to $\mathrm{Mon}(P)$. Moreover, for any $m, n \in \mathrm{Mon}(P)$ and $i, j \geq 0$ one has that $ms^i \prec ns^j$ implies that $m \prec n$ or $i < j$.*

Proof. Suppose $m \prec n$ with $m, n \in \mathrm{Mon}(P)$. Then $sm \prec sn$ that is $m^s s \prec n^s s$. If $m^s \succeq n^s$ then $m^s s \succeq n^s s$ which is a contradiction. We conclude that $m^s \prec n^s$. Now, assume that $m \succeq n$ and $i \geq j$. We have $ms^i \succeq ms^j \succeq ns^j$. $\square$

Assume now σ be compatible with a monomial ordering $\prec$ of P. We define a total ordering on $\mathrm{Mon}(S)$ by putting $ms^i \prec' ns^j$ if and only if $i < j$, or $i = j$ and $m \prec n$, for all $m, n \in \mathrm{Mon}(P)$ and $i, j \geq 0$. Clearly, the restriction of $\prec'$ to $\mathrm{Mon}(P)$ is $\prec$.

Proposition 3.8. *The ordering $\prec'$ is a monomial ordering on S that extends $\prec$.*

Proof. Clearly, an infinite descending sequence in $\mathrm{Mon}(S)$ implies an infinite descending sequence in $\mathrm{Mon}(P)$ which contradicts the condition that $\prec$ is a well-ordering. Let $ms^i, ns^j \in \mathrm{Mon}(S)$ and suppose $ms^i \prec ns^j$ that is $i < j$, or $i = j$ and $m \prec n$. Let $qs^k \in \mathrm{Mon}(S)$ and consider right multiplications $ms^i qs^k = mq^{s^i} s^{i+k}$ and $ns^j qs^k = nq^{s^j} s^{j+k}$. If $i < j$ then $i + k < j + k$. If $i = j$ and $m \prec n$ then $mq^{s^i} \prec nq^{s^i} = nq^{s^j}$. We conclude in both cases that $mq^{s^i} s^{i+k} \prec nq^{s^j} s^{j+k}$. For left multiplications $qs^k ms^i = qm^{s^k} s^{k+i}$ and $qs^k ns^j = qn^{s^k} s^{k+j}$, note that $m \prec n$ implies that $m^{s^k} \prec n^{s^k}$. Then, one may argue in a similar way as for right multiplications. $\square$

Clearly, a byproduct of Proposition 3.7 and Proposition 3.8 is that there exist monomial orderings on the skew polynomial ring S if and only if σ is compatible with a monomial ordering of P. Note that $\prec'$ is well-known as module ordering when we consider S as a free P-module. Moreover, by Proposition 3.7 it follows also that the monomial ordering of S is uniquely defined by the one of P when one compares monomials of the same s-degree.

From now on, *we assume* S be endowed with a monomial ordering $\prec$.

Definition 3.9. *Let $f \in S, f = \sum_i \alpha_i m_i s^i$ with $m_i \in \mathrm{Mon}(P), \alpha_i \in K^*$. Then, we denote $\mathrm{lm}(f) = m_k s_k = \max_{\prec}\{m_i s^i\}$, $\mathrm{lc}(f) = \alpha_k$ and $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f)$. If $G \subset S$ we put $\mathrm{lm}(G) = \{\mathrm{lm}(f) \mid f \in G, f \neq 0\}$. We denote as $\mathrm{LM}(G)$ and $\mathrm{LM}_l(G)$ respectively the two-sided ideal and the left ideal of S generated by $\mathrm{lm}(G)$. Moreover, we denote by $\mathrm{LM}_P(G)$ the P-submodule of S generated by $\mathrm{lm}(G)$.*

Proposition 3.10. *Let J be an ideal (respectively left ideal) of S. Then, the set $\{w+J \mid w \in \mathrm{Mon}(S) \setminus \mathrm{LM}(J)\}$ (resp. $\{w+J \mid w \in \mathrm{Mon}(S) \setminus \mathrm{LM}_l(J)\}$) is a K-basis of the space S/J. If $J \subset S$ is a P-submodule, in the same way one defines the K-basis $\{w+J \mid w \in \mathrm{Mon}(S) \setminus \mathrm{LM}_P(J)\}$.*

Proof. Let $w \in \mathrm{Mon}(S)$. By induction on the monomial ordering of S, we can assume that for any monomial $v \in \mathrm{Mon}(S)$ such that $v \prec w$ there is a polynomial $f \in S$ belonging to the span of $N = \mathrm{Mon}(S) \setminus \mathrm{LM}(J)$ such that $v - f \in J$. If $w \notin N$ then there is $g \in J$ such that $w = p\mathrm{lm}(g)q$ with $p, q \in \mathrm{Mon}(S)$. Therefore $f = w - (1/\mathrm{lc}(g))pgq$ is such that $\mathrm{lm}(f) \prec w$ and by induction $f - f' \in J$ for some $f' \in \langle N \rangle_K$. We conclude that $w - f' \in J$. Finally if $f \in N \cap J$ then necessarily $f = 0$. Mutatis mutandis one proves the remaining assertions. □

Definition 3.11. *Let J be an ideal (respectively left ideal) of S and $G \subset J$. We call G a* Gröbner basis (resp. left basis) *of J if $\mathrm{LM}(G) = \mathrm{LM}(J)$ (resp. $\mathrm{LM}_l(G) = \mathrm{LM}_l(J)$). As usual, if J is a P-submodule of S then G is a* Gröbner P-basis *of J when $\mathrm{LM}_P(G) = \mathrm{LM}_P(J)$.*

Proposition 3.12. *Let J be an ideal (respectively left ideal) of S and $G \subset J$. The following conditions are equivalent:*

(i) *G is a Gröbner basis (resp. left basis) of J;*
(ii) *for any $f \in J$, one has a* Gröbner representation of f with respect to G *that is $f = \sum_i f_i g_i h_i$ (resp. $f = \sum_i f_i g_i$) with $\mathrm{lm}(f) \succeq \mathrm{lm}(f_i)\mathrm{lm}(g_i)\mathrm{lm}(h_i)$ (resp. $\mathrm{lm}(f) \succeq \mathrm{lm}(f_i)\mathrm{lm}(g_i)$) and $f_i, h_i \in S$, for all i.*

A similar characterization holds for Gröbner P-bases.

Proof. It follows immediately by the reduction process which is implicit in the proof of Proposition 3.10. □

Proposition 3.13. *Let J be a graded ideal of S and $G \subset J$ be a subset of s-homogeneous elements. The following conditions are equivalent:*

(i) *G is a Gröbner basis of J;*
(ii) *$G\,\Sigma$ is a Gröbner left basis of J;*
(iii) *$\Sigma\, G\, \Sigma$ is a Gröbner P-basis of J.*

Proof. Assume $G = \{g_i\}$ is a Gröbner basis of J and put $d_i = \deg_s(g_i)$. If $f \in J$ then one has $f = \sum_i f_i g_i h_i$ where $f_i, h_i \in S$ and $\mathrm{lm}(f) \succeq \mathrm{lm}(f_i)\mathrm{lm}(g_i)\mathrm{lm}(h_i)$, for all i. Decompose $h_i = \sum_j h_{ij} s^j$ with $h_{ij} \in P$ for any i, j. Then, we have $\mathrm{lm}(f) \succeq \mathrm{lm}(f_i)\mathrm{lm}(g_i)\mathrm{lm}(h_{ij})s^j$, for all i, j. Since $\mathrm{lm}(g_i)$ has s-degree d_i, one obtains $\mathrm{lm}(f_i)\mathrm{lm}(g_i)\mathrm{lm}(h_{ij})s^j = \mathrm{lm}(f_i)\mathrm{lm}(h_{ij})^{s^{d_i}}\mathrm{lm}(g_i s^j)$. Moreover, as in Proposition 2.3, we have $f = \sum_{i,j} f_i g_i h_{ij} s^j = \sum_{i,j} f_i h_{ij}^{s^{d_i}} g_i s^j$. From σ compatible with $\prec$ it follows that $\mathrm{lm}(h_{ij}^{s^{d_i}}) = \mathrm{lm}(h_{ij})^{s^{d_i}}$ and hence f has a left Gröbner representation with respect to $G\,\Sigma$, that is this set is a left Gröbner basis of J. The rest of the proof is straightforward. □

4. Buchberger algorithm

After Proposition 3.13, in order to obtain a homogeneous Gröbner basis G of a (two-sided) graded ideal $J \subset S$ one has to start with a homogeneous generating set H and consider the P-basis $H' = \Sigma\, H\, \Sigma$. Then, one should transform H' into a homogeneous Gröbner P-basis G' of J and finally reduce G' as $G' = \Sigma\, G\, \Sigma$ with

$G \subset J$. Apart with problems concerning termination of the module Buchberger algorithm (P is not Noetherian and S is a P-module of countable rank) that we will show solvable for the truncated algorithm up to some s-degree (see Proposition 4.7), it is more desirable to have a procedure able to compute G without actually considering all elements of G'. To obtain this, we need an additional requirement for the endomorphism σ.

Note that, since $\sigma : P \to P$ is a ring homomorphism, such map is increasing with respect to the divisibility relation in P, that is $f \mid g$ implies that $f^s \mid g^s$ and in this case $(g/f)^s = g^s/f^s$ with $f, g \in P$.

Proposition 4.1. *The following conditions are equivalent:*

(a) $\gcd(x_i^s, x_j^s) = 1$*, for all* $i \neq j$*;*
(b) $\gcd(m^s, n^s) = \gcd(m, n)^s$*, for all* $m, n \in \mathrm{Mon}(P)$.

Moreover, in this case one has $m \mid n$ *if and only if* $m^s \mid n^s$ *and* $\mathrm{lcm}(m^s, n^s) = \mathrm{lcm}(m, n)^s$ *with* $m, n \in P$*. In other words,* σ *is a lattice homomorphism with respect to the divisibility relation in* $\mathrm{Mon}(P)$.

Proof. Assume (a) and let $m, n \in \mathrm{Mon}(P)$ such that $\gcd(m, n) = 1$. If $m = x_{i_1} \cdots x_{i_k}$ and $n = x_{j_1} \cdots x_{j_l}$ then $m^s = x_{i_1}^s \cdots x_{i_k}^s$ and $n^s = x_{j_1}^s \cdots x_{j_l}^s$ with $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$. Since $\gcd(x_i^s, x_j^s) = 1$ for all $i \neq j$, we conclude that $\gcd(m^s, n^s) = 1$. Assume now $\gcd(m, n) = u$ and hence $\gcd(m/u, n/u) = 1$. Then $\gcd(m^s/u^s, n^s/u^s) = \gcd((m/u)^s, (m/u)^s) = 1$ and therefore $\gcd(m^s, n^s) = u^s$ that is (b) holds. Suppose $m^s \mid n^s$ that is $m^s = \gcd(m^s, n^s) = \gcd(m, n)^s$. Since σ is injective we have that $m = \gcd(m, n)$ that is $m \mid n$. Moreover, one obtains $\mathrm{lcm}(m, n)^s = (mn/\gcd(m, n))^s = (mn)^s/\gcd(m, n)^s = m^s n^s/\gcd(m^s, n^s) = \mathrm{lcm}(m^s, n^s)$ for all $m, n \in \mathrm{Mon}(P)$. □

Definition 4.2. *We say that* σ is compatible with divisibility in $\mathrm{Mon}(P)$ *if for all* $i \neq j$*, one has* $\gcd(x_i^s, x_j^s) = 1$ *that is the variables occuring in the monomials* x_i^s, x_j^s *are disjoint.*

Note that if a monomial endomorphism of P is compatible with divisibility then it is automatically injective since the monomials x_i^s are algebraically independent. Let $\mid$ be the divisibility relation and $\prec$ a monomial ordering on $\mathrm{Mon}(P)$. From now on, *we assume* that the monomial endomorphism $\sigma : P \to P$ is compatible both with $\mid$ and with $\prec$.

We recall now some basic results in the theory of module Gröbner bases by applying them to the free P-module S whose (left) free basis is $\Sigma = \{s^i\}_{i \geq 0}$. Consider $f, g \in S \setminus \{0\}$ two elements whose leading monomials have the same s-degree (component), that is $\mathrm{lm}(f) = ms^i, \mathrm{lm}(g) = ns^i$ with $m, n \in \mathrm{Mon}(P)$ and $i \geq 0$. If we put $\mathrm{lc}(f) = \alpha, \mathrm{lc}(g) = \beta$ and $l = \mathrm{lcm}(m, n)$, one defines the *S-polynomial* $\mathrm{spoly}(f, g) = (l/\alpha m)f - (l/\beta n)g$. Clearly $\mathrm{spoly}(f, g) = -\mathrm{spoly}(g, f)$ and $\mathrm{spoly}(f, f) = 0$.

Proposition 4.3 (Buchberger criterion)**.** *Let* G *be a generating set of a* P*-submodule* $J \subset S$*. Then* G *is a Gröbner basis of* J *if and only if for all* $f, g \in G \setminus \{0\}$ *such that* $\deg_s(\mathrm{lm}(f)) = \deg_s(\mathrm{lm}(g))$*, the S-polynomial* $\mathrm{spoly}(f, g)$ *has a Gröbner representation with respect to* G.

Usually the above result, see for instance [9, 14], is stated when P is a polynomial ring with a finite number of variables and S is a P-module of finite rank. In fact such assumptions are not needed since Noetherianity is not used in the proof, but only the existence of a monomial ordering for the ring P and the free module S. See also the comprehensive Bergman's paper [2] where the "Diamond Lemma" is proved without any restriction on the finiteness of the variable set. In the following results we show how the Buchberger criterion, and hence the corresponding algorithm, can be reduced up to the symmetry defined by the monoid Σ on S.

Lemma 4.4. *Let $f, g \in S \setminus \{0\}$ and let $i \leq j$ such that $\deg_s(lm(f)) + i = \deg_s(\mathrm{lm}(g)) + j$. Then $\mathrm{spoly}(s^i f, s^j g) = s^i \mathrm{spoly}(f, s^{j-i} g)$ and $\mathrm{spoly}(f s^i, g s^j) = \mathrm{spoly}(f, g s^{j-i}) s^i$.*

Proof. Let $\mathrm{lt}(f) = \alpha m s^k, \mathrm{lt}(g) = \beta n s^l$ with $\alpha, \beta \in K^*$ and $m, n \in \mathrm{Mon}(P)$. Then $\mathrm{lt}(s^i f) = \alpha m^{s^i} s^{i+k}, \mathrm{lt}(s^j g) = \beta n^{s^j} s^{j+l}$ and $\mathrm{lt}(s^{j-i} g) = \beta n^{s^{j-i}} s^{j-i+l}$. By compatibility of σ with divisibility in $\mathrm{Mon}(P)$, if $q = \mathrm{lcm}(m, n^{s^{j-i}})$ then $\mathrm{lcm}(m^{s^i}, n^{s^j}) = q^{s^i}$. Therefore $h = \mathrm{spoly}(f, s^{j-i} g) = (q/\alpha m) f - (q/\beta n^{s^{j-i}}) s^{j-i} g$ and hence we have $s^i h = (q^{s^i}/\alpha m^{s^i}) s^i f - (q^{s^i}/\beta n^{s^j}) s^j g = \mathrm{spoly}(s^i f, s^i g)$.

Note now that $\mathrm{lt}(f s^i) = \alpha m s^{i+k}, \mathrm{lt}(g s^j) = \beta n s^{j+l}$ and $\mathrm{lt}(g s^{j-i}) = \beta n s^{j-i+l}$. If $q = \mathrm{lcm}(m, n)$ and $h = \mathrm{spoly}(f, g s^{j-i}) = (q/\alpha m) f - (q/\beta n) g s^{j-i}$ we have simply that $h s^i = (q/\alpha m) f s^i - (q/\beta n) g s^j = \mathrm{spoly}(f s^i, g s^j)$. □

Proposition 4.5 (Two-sided Σ-criterion)**.** *Let G be an s-homogeneous basis of a graded two-sided ideal $J \subset S$. Then G is a Gröbner basis of J if and only if for all $f, g \in G \setminus \{0\}$ and for any $i, j \geq 0$, the S-polynomials $\mathrm{spoly}(f, s^i g s^j)$ ($\deg_s(f) = \deg_s(g) + i + j$) and $\mathrm{spoly}(f s^i, s^j g)$ ($\deg_s(f) + i = \deg_s(g) + j$) have a Gröbner representation with respect to $\Sigma\, G\, \Sigma$.*

Proof. By Proposition 3.13 we have to prove that $G' = \Sigma\, G\, \Sigma$ is a Gröbner basis of J as P-module, that is G' is P-basis of J and the S-polynomials $h = \mathrm{spoly}(s^i f s^k, s^j g s^l)$ have a Gröbner representation with respect to G' for all $f, g \in G \setminus \{0\}$ and for any $i, j, k, l \geq 0$ such that $\deg_s(f) + i + k = \deg_s(g) + j + l$. Since G is a homogeneous basis of J as two-sided ideal, from Proposition 2.3 it follows that G' is a generating set of J' as P-module. Consider now all possibilities $i \leq j$ or $i \geq j$ and $k \leq l$ or $k \geq l$ and apply Lemma 4.4. If $i \leq j, k \leq l$ one has $h = s^i \mathrm{spoly}(f, s^{j-i} g s^{l-k}) s^k$, if $i \leq j, k \geq l$ then $h = s^i \mathrm{spoly}(f s^{l-k}, s^{j-i} g) s^l$, and so on. Then, assume that a S-polynomial $h = \mathrm{spoly}(f, g)$, with $f, g \in G' \setminus \{0\}$, has a Gröbner representation with respect to G' as P-basis of J, that is $h = \sum_i f_i g_i$ with $f_i \in P, g_i \in G'$ and $\mathrm{lm}(h) \geq \mathrm{lm}(f_i)\mathrm{lm}(g_i)$, for all i. We have to prove that $s^k h s^l$ has also a Gröbner representation with respect to G' for any $k, l \geq 0$. One has that $s^k h s^l = \sum_i f_i^{s^k} s^k g_i s^l$ and $\mathrm{lm}(s^k h s^l) = s^k \mathrm{lm}(h) s^l \geq s^k \mathrm{lm}(f_i)\mathrm{lm}(g_i) s^l = \mathrm{lm}(f_i)^{s^k} s^k \mathrm{lm}(g_i) s^l = \mathrm{lm}(f_i^{s^k})\mathrm{lm}(s^k g_i s^l)$. Since $s^k g_i s^l \in G' = \Sigma\, G\, \Sigma$, one obtains that $s^k h s^l$ has a Gröbner representation with respect to G'. □

In analogy with the theory of Gröbner bases for the free associative algebra, see Section 6, we call $\mathrm{spoly}(f, s^i g s^j)$ the *inclusion S-polynomials* of the pair (f, g) and $\mathrm{spoly}(f s^i, s^j g)$ the *overlapping S-polynomials* of (f, g), for all suitable i, j. A criterion similar to Proposition 4.5 holds clearly for Gröbner left bases of left ideals of S where no restriction about the s-homogeneity of bases and ideals is needed.

Proposition 4.6 (Left Σ-criterion)**.** *Let G be a basis of a left ideal $J \subset S$. Then G is a Gröbner basis of J if and only if for all elements $f, g \in G \setminus \{0\}$ such that*

$i = \deg_s(\mathrm{lm}(f)) - \deg_s(\mathrm{lm}(g)) \geq 0$, *the S-polynomial* $\mathrm{spoly}(f, s^i g)$ *has a Gröbner representation with respect to* ΣG.

A standard procedure in the (module) Buchberger algorithm is the following.

Algorithm 4.1 Reduce

Input: $G \subset S$ and $f \in S$.
Output: $h \in S$ such that $f - h \in \langle G \rangle_P$ and $h = 0$ or $\mathrm{lm}(h) \notin \mathrm{LM}_P(G)$.
$h := f$;
while $h \neq 0$ and $\mathrm{lm}(h) \in \mathrm{LM}_P(G)$ **do**
  choose $g \in G, g \neq 0$ such that $\mathrm{lm}(g)$ P-divides $\mathrm{lm}(h)$;
  $h := h - (\mathrm{lt}(h)/\mathrm{lt}(g))g$;
end while;
return h.

Note that if $\mathrm{lt}(g) = \alpha m s^i, \mathrm{lt}(h) = \beta n s^i$ with $\alpha, \beta \in K^*$ and $m, n \in \mathrm{Mon}(P)$, by definition $\mathrm{lt}(h)/\mathrm{lt}(g) = (\alpha m)/(\beta n)$. Moreover, the termination of REDUCE is provided since $\prec$ is a well-ordering on $\mathrm{Mon}(S)$. In particular, even if G is an infinite set, there are only a finite number of elements $g \in G, g \neq 0$ such that $\mathrm{lm}(g)$ P-divides $\mathrm{lm}(h)$ and hence $\mathrm{lm}(g) \preceq \mathrm{lm}(h)$.

It is well-known that if $\textsc{Reduce}(f, G) = 0$ then f has a Gröbner representation with respect to G. Moreover, if $\textsc{Reduce}(f, G) = h \neq 0$ then clearly we have $\textsc{Reduce}(f, G \cup \{h\}) = 0$. Therefore, from Proposition 4.5 it follows immediately the correctness of the following algorithm.

Algorithm 4.2 SKEWGBASIS

Input: H, an s-homogeneous basis of a graded two-sided ideal $J \subset S$.
Output: G, an s-homogeneous Gröbner basis of J.
$G := H$;
$B := \{(f, g) \mid f, g \in G\}$;
while $B \neq \emptyset$ **do**
  choose $(f, g) \in B$;
  $B := B \setminus \{(f, g)\}$;
  for all $i, j \geq 0$ such that $i + j = \deg_s(f) - \deg_s(g)$ **do**
    $h := \textsc{Reduce}(\mathrm{spoly}(f, s^i g s^j), \Sigma\, G\, \Sigma)$;
    if $h \neq 0$ **then**
      $B := B \cup \{(g, h), (h, g), (h, h) \mid g \in G\}$;
      $G := G \cup \{h\}$;
    end if;
  end for;
  for all $i, j \geq 0$ such that $j - i = \deg_s(f) - \deg_s(g)$ **do**
    $h := \textsc{Reduce}(\mathrm{spoly}(f s^i, s^j g), \Sigma\, G\, \Sigma)$;
    if $h \neq 0$ **then**
      $B := B \cup \{(g, h), (h, g), (h, h) \mid g \in G\}$;
      $G := G \cup \{h\}$;
    end if;
  end for;
end while;
return G.

Clearly, all well-known criteria (product criterion, chain criterion, etc) can be applied to SkewGBasis to shorten the number of S-polynomials to be considered. In fact, this algorithm can be understood as the usual (module) Buchberger procedure applied to the P-basis $\Sigma\, H\, \Sigma$, where an additional criterion to avoid "useless pairs" is provided by Proposition 4.5. Note that owing to Proposition 4.6, one has also a similar algorithm for computing a Gröbner left basis of any left ideal of S. About the termination of the algorithm SkewGBasis we have the following result.

Proposition 4.7. *Let $J \subset S$ be a graded two-sided ideal which is finitely generated up to some s-degree $d > 0$. Then, an s-homogeneous Gröbner basis of J up to degree d is also finite. In other words, if we consider a selection strategy for the S-polynomials based on their s-degree, we obtain that the d-truncated version of the algorithm* SkewGBasis *terminates in a finite number of steps.*

Proof. Let H_d be a finite s-homogeneous generating set of J up to degree d. Denote $\Sigma_d = \{s^i\}_{i\leq d}$ and put $H'_d = \Sigma_d H_d \Sigma_d$. Since H'_d is also a finite set, consider X_d the finite set of variables of P occurring in the elements of H'_d and define $P^{(d)} = K[X_d]$ and $S^{(d)} = \bigoplus_{i\leq d} P^{(d)} s^i$. In fact, the d-truncated algorithm SkewGBasis computes a subset of a Gröbner basis up to degree d of the $P^{(d)}$-submodule $J^{(d)} \subset S^{(d)}$ generated by H'_d. By Noetherianity of the ring $P^{(d)}$ and the free $P^{(d)}$-module $S^{(d)}$ which has finite rank, we clearly obtain termination. □

Note that the above result provides algorithmic solution of the membership problem for graded ideals of S which are finitely generated up to any degree.

5. Σ-invariant ideals of P

In this section we define Gröbner bases of Σ-invariant ideals $I \subset P$ which generates I up to the action of Σ. Moreover, if P can be endowed with a suitable grading, we show how such bases can be computed in the algebra S for a class of graded Σ-invariant ideals. As usual, we fix a monomial endomorphism $\sigma : P \to P$ which is compatible both with the divisibility and a monomial ordering on $\mathrm{Mon}(P)$ and we extend this to an ordering on $\mathrm{Mon}(S)$. From Section 2 we know that Σ-invariant ideals of P are just left S-submodules of P. Since we make use of identification $\Sigma = \{s^i\}$, for all $f \in P \subset S$ and for any $i \geq 0$ one has that $s^i \cdot f = f^{s^i} = \sigma^i(f)$ and $s^i f = (s^i \cdot f)s^i$.

Definition 5.1. *Let $I \subset P$ be a Σ-invariant ideal and $G \subset I$. We say that G is a* Σ-basis *of I if G is a basis of I as left S-module. In other words, $\Sigma \cdot G$ is a basis of I as P-ideal.*

Proposition 5.2. *Let $G \subset P$. Then $\mathrm{lm}(\Sigma \cdot G) = \Sigma \cdot \mathrm{lm}(G)$. In particular, if I is a Σ-invariant P-ideal then $\mathrm{LM}_P(I)$ is also Σ-invariant.*

Proof. Since σ is compatible with the monomial ordering of P, it is sufficient to note that $\mathrm{lm}(s^i \cdot f) = s^i \cdot \mathrm{lm}(f)$ for any $f \in P$ and $i \geq 0$. □

Definition 5.3. *Let $I \subset P$ be a Σ-invariant ideal and $G \subset I$. We call G a* Gröbner Σ-basis *of I if $\mathrm{lm}(G)$ is a basis of $\mathrm{LM}_P(I)$ as left S-module. In other words, $\Sigma \cdot G$ is a Gröbner basis of I as P-ideal.*

The computation of Gröbner Σ-bases of Σ-invariant P-ideals is relevant, for instance, in applications to difference algebra (cf. [18], Chapter 3). Such computations appear also in other contexts, see for instance [8] and [3]. Note that in the latter paper Gröbner Σ-bases are named "equivariant Gröbner bases".

In analogy with Proposition 4.5 and Proposition 4.6, we present here a Σ-criterion that allows to reduce the number of S-polynomials to be checked to provide that a Σ-basis is of Gröbner type.

Proposition 5.4 (Σ-criterion in P)**.** *Let G be a Σ-basis of a Σ-invariant ideal $I \subset P$. Then G is a Gröbner Σ-basis of I if and only if for all $f, g \in G \setminus \{0\}$ and for any $i \geq 0$, the S-polynomial* $\mathrm{spoly}(f, s^i \cdot g)$ *has a Gröbner representation with respect to $\Sigma \cdot G$.*

Proof. Consider any pair of elements $s^i \cdot f, s^j \cdot g \in \Sigma \cdot G$ $(f, g \in G)$ and let $i \leq j$. By compatibility of σ with divisibility in $\mathrm{Mon}(P)$ (cf. Lemma 4.4), one has that $\mathrm{spoly}(s^i \cdot f, s^j \cdot g) = s^i \cdot \mathrm{spoly}(f, s^k \cdot g)$ with $k = j - i$. Assume that $\mathrm{spoly}(f, s^k \cdot g) = h = \sum_l f_l (s^l \cdot g_l)$ $(f_l \in P, g_l \in G)$ is a Gröbner representation with respect to $\Sigma \cdot G$. Since the endomorphism σ is compatible with the monomial ordering of P, we have also the Gröbner representation $\mathrm{spoly}(s^i \cdot f, s^j \cdot g) = s^i \cdot h = \sum_l (s^i \cdot f_l)(s^{i+l} \cdot g_l)$. $\square$

Note that some version of this criterion can be found in [3], Theorem 2.5, where it is called "equivariant Buchberger criterion". Before than this, the same ideas have been used in [17] for the Proposition 3.11. From this criterion it follows immediately the correctness of the following algorithm.

Algorithm 5.1 SigmaGBasis

Input: H, a Σ-basis of a Σ-invariant ideal $I \subset P$.
Output: G, a Gröbner Σ-basis of I.
$G := H$;
$B := \{(f, g) \mid f, g \in G\}$;
while $B \neq \emptyset$ **do**
    choose $(f, g) \in B$;
    $B := B \setminus \{(f, g)\}$;
    for all $i \geq 0$ **do**
        $h := \textsc{Reduce}(\mathrm{spoly}(f, s^i \cdot g), \Sigma \cdot G)$;
        if $h \neq 0$ **then**
            $B := B \cup \{(g, h), (h, g), (h, h) \mid g \in G\}$;
            $G := G \cup \{h\}$;
        end if;
    end for;
end while;
return G.

As for the algorithm SkewGBasis, all criteria to avoid useless pairs can be added to SigmaGBasis. Note that termination of this algorithm is not provided in general and this is, in fact, one of the main problems in applications to differential/difference algebra. Nevertheless, in what follows we describe some family of Σ-invariant ideals of P where a truncated version of the algorithm SigmaGBasis stops in a finite number of steps. Such ideals are in bijective correspondence with a class of graded (two-sided) ideals of S which have truncated termination of SkewGBasis provided by Proposition 4.7.

Consider now the P-module homomorphism $\pi : S \to P$ such that $s^i \mapsto 1$, for all i. Clearly π is a left S-module epimorphism whose kernel is the left ideal of S generated by $s - 1$.

Definition 5.5. *Let J be a graded ideal of S and put $J^P = \pi(J)$. Clearly J^P is a Σ-invariant ideal of P.*

Proposition 5.6. *Let $J \subset S$ be a graded ideal. If G is a homogeneous basis of J then $G^P = \pi(G)$ is a Σ-basis of J^P.*

Proof. Since the map π is a left S-module homomorphism, it is sufficient to note that $G\,\Sigma$ is a left basis of J and $\pi(G\,\Sigma) = \pi(G) = G^P$. ☐

Consider the set of natural numbers $\mathbb{N}$ be endowed with the additional monoid structure defined by putting $x \oplus y = \max(x, y)$, for all $x, y \in \mathbb{N}$. Denote $M = \mathrm{Mon}(P)$ the set of monomials of the polynomial ring P. From now on, *we assume* that there exists a function $\mathrm{w} : M \to \mathbb{N}$ such that for all $m, n \in M$ one has

(i) $\mathrm{w}(1) = 0, \mathrm{w}(m) > 0$ if $m \neq 1$;
(ii) $\mathrm{w}(mn) = \mathrm{w}(m) \oplus \mathrm{w}(n)$;
(iii) $\mathrm{w}(s \cdot m) = \mathrm{w}(m) + 1$ for $m \neq 1$.

In other words, if $m = x_{i_1} \cdots x_{i_d}$ with $\mathrm{w}(x_{i_1}) \leq \ldots \leq \mathrm{w}(x_{i_d})$ then $\mathrm{w}(m) = \mathrm{w}(x_{i_d})$. Note that condition (iii) implies that $s \cdot m \neq m$ for any monomial $m \neq 1$. We put $M_i = \{m \in M \mid \mathrm{w}(m) = i\}$ for all $i \in \mathbb{N}$ and define $P_i \subset P$ the subspace spanned by M_i. We have that $P_0 = K$. Clearly $P = \bigoplus_i P_i$ is a grading of the algebra P defined by the monoid $(\mathbb{N}, \oplus)$ by means of the function w. Note that the set $\Sigma = \langle\sigma\rangle$ can be identified with $\mathbb{N}$ since the map σ has infinite order. Moreover, by (iii) we have compatibility between the gradings $S = \bigoplus S_i$ $(S_i = Ps^i)$ and $P = \bigoplus_i P_i$ with respect to left S-module structure of P.

Definition 5.7. *We call a function* $\mathrm{w} : M \to \mathbb{N}$ *satisfying conditions (i)–(iii) a* weight function of P endowed with σ. *Then, an element $f \in P_i$ is said* w-homogeneous of weight i.

Weight functions naturally arise in the following relevant examples.

- Let $P = K[X] = K[x_1, x_2, \ldots]$ and define $\sigma : P \to P$ the algebra monomorphism of infinite order such that $\sigma(x_i) = x_{i+1}$, for all i. Clearly σ is a monomial map compatible with divisibility in $\mathrm{Mon}(P)$ and many usual monomial orderings on P, like lex, degrevlex, etc, are compatible with σ. By denoting $u = x_1$ we have that $P = K[u, \sigma u, \sigma^2 u, \ldots]$ which is called the *ring of ordinary difference polynomials* and used in the theory of difference algebras (see [18]) for applications to solution of systems of (nonlinear) difference equations. For the ring P endowed with the shift operator σ we can clearly define the weight function $\mathrm{w}(x_i) = i$, for any i.

- Consider the polynomial ring $P = K[X \times \mathbb{N}^*]$ and denote $x_i(j)$ each variable (x_i, j). Let $\sigma : P \to P$ the monomorphism such that $\sigma(x_i(j)) = x_i(j+1)$, for all i, j. In Section 6 we show how to embed the free associative algebra $K\langle X\rangle$ into the skew polynomial ring defined by P and σ. Note that we have the weight function $\mathrm{w}(x_i(j)) = j$, for any i, j.

Definition 5.8. *Let I be a Σ-invariant ideal of P. We call I* w-graded *if $I = \sum_i I_i$ with $I_i = I \cap P_i$. In this case, one has that $s \cdot I_i \subset I_{i+1}$ for $i > 0$.*

The existence of a weight function implies that one has a homogeneous injective linear map $\xi : P \to S$ such that $f \mapsto fs^i$, for all $f \in P_i$. Note that $\pi\xi = id$ and $\xi(s \cdot f) = s\xi(f)$, for any $f \in P_i, i > 0$.

Definition 5.9. *Let I be a* w*-graded Σ-invariant ideal of P and consider the graded left ideal $\xi(I) \subset S$. Denote by I^S the graded (two-sided) ideal of S generated by $\xi(I)$. In other words, if $G = \{fs^i \mid f \in I_i, i \geq 0\}$ then I^S is left ideal generated by $G\Sigma = \{fs^j \mid f \in I_i, j \geq i \geq 0\}$ or equivalently I^S has the basis $\Sigma G \Sigma$ as P-submodule of S. We call I^S the* skew analogue *of I.*

Proposition 5.10. *Let $I \subset P$ be a* w*-graded Σ-invariant ideal. Then $I^{SP} = I$, that is there is a* bijective correspondence *between all* w*-graded Σ-invariant ideals of P and their skew analogues in S.*

Proof. Put $J = I^{SP} = \pi(I^S)$. For any $f \in I_i$ and $j \geq i$ we have clearly $\pi(fs^j) = f$. Since the elements fs^j are a left basis of I^S, the ideal I is Σ-invariant and π is a left S-module homomorphism, we have that $J \subset I$. Moreover, the elements f are a basis of $I = \sum_i I_i$ and one has also that $I \subset J$. □

The next propositions need the following lemmas.

Lemma 5.11. *If $s^k \cdot m$ divides n, with $m, n \in M$, then $\mathrm{w}(n) - k \geq \mathrm{w}(m)$.*

Proof. Since $n = q(s^k \cdot m)$ with $q \in M$, we have $\mathrm{w}(n) \geq \mathrm{w}(s^k \cdot m) = k + \mathrm{w}(m)$. □

Lemma 5.12. *Let $m, n \in M$ and $x_i \in X, x_i \mid m$ such that $\mathrm{w}(m) = \mathrm{w}(x_i)$. If $\mathrm{w}(m) > \mathrm{w}(n)$ then $x_i \nmid n$.*

Proof. Let $m = x_{i_1} \cdots x_{i_k}$ and $n = x_{i_1} \cdots x_{i_l}$ with $\mathrm{w}(x_{i_1}) \leq \ldots \leq \mathrm{w}(x_{i_k})$ and $\mathrm{w}(x_{j_1}) \leq \ldots \leq \mathrm{w}(x_{j_l})$. Then, we have $\mathrm{w}(x_{i_k}) > \mathrm{w}(x_{j_l}) \geq \mathrm{w}(x_{j_\alpha})$ and therefore $x_{i_k} \neq x_{j_\alpha}$, for all $1 \leq \alpha \leq l$. □

Lemma 5.13. *Let $m, n \in M$ and put $l = \mathrm{lcm}(m, n)$. Then, one has that $\mathrm{w}(l) = \mathrm{w}(m) \oplus \mathrm{w}(n)$.*

Proof. Let $l = pm = qn$ with $p, q \in M$ and then $\mathrm{w}(l) = \mathrm{w}(p) \oplus \mathrm{w}(m) = \mathrm{w}(q) \oplus \mathrm{w}(n)$. By Lemma 5.12, if $\mathrm{w}(l) = \mathrm{w}(p) > \mathrm{w}(m)$ then there is a variable $x_i \mid l$ such that $\mathrm{w}(l) = \mathrm{w}(x_i)$ and $x_i \nmid m$. Therefore, one has necessarily that $x_i \mid n$ and hence $\mathrm{w}(l) = \mathrm{w}(n)$. □

Proposition 5.14. *Let I be a* w*-graded Σ-invariant P-ideal, then I^S is a graded ideal of S. Let $G = \bigcup_i G_i$ be a* w-homogeneous *Σ-basis of I that is $G_i \subset I_i$. Then $G^S = \{fs^i \mid f \in G_i, i \geq 0\}$ is an s-homogeneous basis of I^S.*

Proof. Consider the elements fs^j with $f \in I_i, j \geq i$ which form a left basis of I^S. Since G is a Σ-basis, one has $f = \sum_k f_k(s^k \cdot g_k)$ with $f_k \in P, g_k \in G_{i_k}$. From $\mathrm{w}(f) = i$, by Lemma 5.11 we obtain that $i - k \geq i_k$. We have therefore that

$fs^j = \sum_k f_k(s^k \cdot g_k)s^k s^{j-k} = \sum_k f_k s^k(g_k s^{j-k})$ with $j - k \geq i - k \geq i_k$ and hence $g_k s^{j-k} \in G^S\,\Sigma$, for all k. ☐

Note now that by Proposition 3.7 we have that $ms^i \prec ns^i$ if and only if $m \prec n$, for all $m, n \in M$ and for any $i \geq 0$. In other words, if fs^i ($f \in P$) is an s-homogeneous element of S then $\mathrm{lm}(fs^i) = \mathrm{lm}(f)s^i$.

Lemma 5.15. *Let $I \subset P$ be a* w*-graded Σ-invariant ideal. If $G = \bigcup_i I_i$, by definition I^S is the graded ideal of S generated by G^S. Then G^S is an s-homogeneous Gröbner basis of I^S.*

Proof. Let $fs^i, gs^j \in G^S\,\Sigma$ that is the w-homogeneous elements $f, g \in G$ are such that $i \geq \mathrm{w}(f), j \geq \mathrm{w}(g)$. Assume $i \geq j$ and put $k = i - j$. By Proposition 4.6 we have to check for Gröbner representations of the S-polynomial $\mathrm{spoly}(fs^i, s^k gs^j)$ with respect to $\Sigma\, G^S\, \Sigma$. Since G is clearly a Gröbner Σ-basis of I, one has that the S-polynomial $\mathrm{spoly}(f, s^k \cdot g)$ has a Gröbner representation with respect to $\Sigma \cdot G$, say $h = \mathrm{spoly}(f, s^k \cdot g) = \sum_l f_l(s^l \cdot g_l)$ with $f_l \in P, g_l \in G$. Note that $\mathrm{spoly}(fs^i, s^k gs^j) = hs^i = \sum_l f_l(s^l \cdot g_l)s^i$. We have to prove now that $i \geq l + \mathrm{w}(g_l)$ for any l, because in this case one has the Gröbner representation $hs^i = \sum_l f_l s^l(g_l s^{i-l})$. In fact, by Lemma 5.11 and Lemma 5.13 we have that $\mathrm{w}(f) \oplus \mathrm{w}(g) = \mathrm{w}(h) \geq l + \mathrm{w}(g_l)$. Then, from $i \geq \mathrm{w}(f)$ and $i \geq j \geq \mathrm{w}(g)$ one obtains the claim. ☐

Proposition 5.16. *Let $G \subset \bigcup_i P_i$. Then $\mathrm{lm}(G)^S = \mathrm{lm}(G^S)$. Moreover, if I is a* w*-graded Σ-invariant ideal of P then $\mathrm{LM}_P(I)^S = \mathrm{LM}(I^S)$.*

Proof. If $f \in P$ is a w-homogeneous element then $\mathrm{w}(\mathrm{lm}(f)) = \mathrm{w}(f) = i$ and $\mathrm{lm}(f)s^i = \mathrm{lm}(fs^i)$. We obtain that $\mathrm{lm}(G)^S = \mathrm{lm}(G^S)$. Consider now $G = \bigcup_i I_i$. By definition I^S is the ideal of S generated by G^S. Moreover, since $I = \sum_i I_i$ one has that $\mathrm{lm}(G) = \mathrm{lm}(I)$ and hence $\mathrm{LM}_P(I)^S$ is the ideal generated by $\mathrm{lm}(G)^S = \mathrm{lm}(G^S)$. Finally, by Lemma 5.15 one has that $\mathrm{LM}(I^S)$ is the ideal of S generated by $\mathrm{lm}(G^S)$. ☐

Proposition 5.17. *Let $I \subset P$ be a* w*-graded Σ-invariant ideal. Let $G = \bigcup_i G_i$ be a* w*-homogeneous Gröbner Σ-basis of I. Then, $G^S = \{fs^i \mid f \in G_i\}$ is an s-homogeneous Gröbner basis of I^S.*

Proof. By hypothesis $\mathrm{lm}(G)$ is a Σ-basis of $\mathrm{LM}_P(I)$. Then $\mathrm{lm}(G^S) = \mathrm{lm}(G)^S$ is a basis of $\mathrm{LM}_P(I)^S = \mathrm{LM}(I^S)$ that is G^S is a Gröbner basis of I^S. ☐

Proposition 5.18. *Let I be a* w*-graded Σ-invariant ideal of P. If G is an s-homogeneous Gröbner basis of I^S then $G^P = \pi(G)$ is a Gröbner Σ-basis of I.*

Proof. Let $f \in I_l$ for some $l \geq 0$ and consider the element $fs^l \in I^S$. Since G is an s-homogeneous Gröbner basis of I^S, there is $gs^k \in G$ ($g \in P, k \geq 0$) such that $qs^i\mathrm{lm}(gs^k)s^j = qs^i\mathrm{lm}(g)s^{k+j} = \mathrm{lm}(fs^k) = \mathrm{lm}(f)s^k$ with $q \in M$ and $i, j \geq 0$. It follows that $q(s^i \cdot \mathrm{lm}(g)) = q\mathrm{lm}(s^i \cdot g) = \mathrm{lm}(f)$ with $g \in G^P$ and we conclude that G^P is a Gröbner Σ-basis of I. ☐

Note that Proposition 5.17 and Proposition 5.18 explain that there is a complete equivalence between Gröbner bases computations for w-graded Σ-invariant ideals $I \subset P$ and their skew analogues I^S which are graded two-sided ideals of S. In particular, Gröbner Σ-bases of I can be computed by the algorithm SkewGBasis when applied to I^S. Precisely, if $H = \bigcup_i H_i$ is a w-homogeneous Σ-basis of I and

$G = \textsc{SkewGBasis}(H^S)$ then $G^P = \pi(G)$ is a w-homogeneous Gröbner Σ-basis of I. We may call this procedure SigmaGBasis2.

The following result provides algorithmic solution of the membership problem for a class of Σ-invariant ideals. Note that such kind of results are quite rare, for instance, in the theory of difference ideals.

Proposition 5.19. *Let $I \subset P$ be a* w*-graded Σ-invariant ideal which is finitely Σ-generated up to some weight $d > 0$. Then, a* w*-homogeneous Gröbner Σ-basis of I up to weight d is also finite. In other words, if we consider a selection strategy for the S-polynomials based on their w-degree, we obtain that the d-truncated version of the algorithm* SigmaGBasis *terminates in a finite number of steps.*

Proof. Note that by Lemma 5.13, the S-polynomial h of two w-homogeneous elements $f, g \in P$ is also w-homogeneous with $\mathrm{w}(h) = \mathrm{w}(f) \oplus \mathrm{w}(g)$. Now, let H_d be a finite w-homogeneous basis of I up to weight d. Denote $\Sigma_d = \{s^i\}_{i \leq d}$ and put $H'_d = \Sigma_d \cdot H_d$. Since H'_d is also a finite set, consider X_d the finite set of variables of P occurring in the elements of H'_d and define $P^{(d)} = K[X_d]$. In fact, the d-truncated algorithm SigmaGBasis computes a subset of a Gröbner basis up to weight d of the ideal $I^{(d)}$ of $P^{(d)}$ generated by H'_d. By Noetherianity of the ring $P^{(d)}$, we clearly obtain termination. $\square$

Note that the above result can be obtained also by Proposition 4.7. In fact, if $I \subset P$ is finitely Σ-generated up to weight d then I^S is a graded ideal of S which is finitely generated up to s-degree d. Precisely, if $H = \bigcup_i H_i$ is a w-homogeneous Σ-basis of I and the set $\bigcup_{i \leq d} H_i$ is finite for all d, then $\{f s^i \mid f \in H_i, i \leq d\}$ is a also a finite set that generates I^S up to degree d.

6. The skew letterplace embedding

Let $X = \{x_1, x_2, \ldots\}$ be a finite or countable set of variables and consider $\mathbb{N}^* = \{1, 2, \ldots\}$ the set of positive integers. We denote by $x_i(j)$ each element (x_i, j) of the product set $X \times \mathbb{N}^*$ and define $P = K[X \times \mathbb{N}^*]$ the polynomial ring in the commuting variables $x_i(j)$. Consider the algebra monomorphism of infinite order $\sigma : P \to P$ such that $x_i(j) \mapsto x_i(j+1)$ for all i, j. Note that σ is a monomial map that is compatible with divisibility in $\mathrm{Mon}(P)$. Then, put $S = P[s; \sigma]$ the skew polynomial ring in the variable s defined by P and σ. Finally, let $F = K\langle X \rangle$ denote the free associative algebra generated by X. We consider F as a graded algebra with respect to the total degree. Recall that $S = \bigoplus_{i \in \mathbb{N}} S_i$ is also a graded algebra with $S_i = P s^i$.

Definition 6.1. *Let $A \subset S$ be a K-subalgebra. If A is spanned by a submonoid $M \subset \mathrm{Mon}(S)$ then we call A* a monomial subalgebra of S *and we denote* $\mathrm{Mon}(A) = M$*. In this case, a monomial ordering of S can be restricted to A.*

For instance, P is a monomial subalgebra of S. We have now a result about the possibility to embed the free associative algebra F into the skew polynomial ring S.

Proposition 6.2. *The graded algebra homomorphism $\iota : F \to S, x_i \mapsto x_i(1)s$ is injective. Then, the free associative algebra F is isomorphic to $R = \mathrm{Im}\,\iota$, a graded monomial subalgebra of S.*

Proof. It is sufficient to note that by the commutation rule of the variable s and the definition of the endomorphism σ, any word $x_{i_1} \cdots x_{i_d} \in \mathrm{Mon}(F)$ maps into $x_{i_1}(1) \cdots x_{i_d}(d) s^d \in \mathrm{Mon}(S)$. $\square$

We call S the *skew letterplace algebra* and the algebra monomorphism ι the *skew letterplace embedding*. In Section 7 we will give motivation for such names. Fix now a monomial ordering $\prec$ on the algebra S that is σ is compatible with the restriction of $\prec$ to $\mathrm{Mon}(P)$. It is easy to show that many usual monomial orderings on P (lex, degrevlex, etc) satisfy such condition. Recall that by the Higman lemma, to define a monomial ordering on P one has to avoid infinite descending sequences for the double-indexed variables $x_i(j)$. In other words, we may put $x_i(j) \prec x_k(l)$ if and only if $i + j < k + l$ or $i + j = k + l, i < k$.

The algebra P has also a multigrading which is defined as follows. If $m = x_{i_1}(j_1) \cdots x_{i_d}(j_d) \in \mathrm{Mon}(P)$, then we denote $\partial(m) = \mu = (\mu_k)_{k \in \mathbb{N}^*}$ where $\mu_k = \#\{\alpha \mid j_\alpha = k\}$. If $P_\mu \subset P$ is the subspace spanned by all monomials of multidegree μ then $P = \bigoplus_\mu P_\mu$ is clearly a multigrading of the algebra P. If $\mu = (\mu_k)$ is a multidegree, we denote $i \cdot \mu = (\mu_{k-i})_{k \in \mathbb{N}^*}$ where we put $\mu_{k-i} = 0$ when $k - i < 1$. By definition of the map σ, if we denote $S_{\mu,i} = P_\mu s^i$ one obtains that $S = \bigoplus_{\mu,i} S_{\mu,i}$ and $S_{\mu,i} S_{\nu,j} \subset S_{\mu+(i\cdot\nu),i+j}$. The elements of each subspace $S_{\mu,i} \subset S$ are said *multi-homogeneous*. An ideal $J \subset S$ is called *multigraded* if $J = \sum_{\mu,i} J_{\mu,i}$ with $J_{\mu,i} = J \cap S_{\mu,i}$. In other words, the ideal J is generated by multi-homogeneous elements. For any integer $i \geq 0$ we denote by 1^i the multidegree $\mu = (\mu_k)_{k \in \mathbb{N}^*}$ such that $\mu_k = 1$ if $k \leq i$ and $\mu_k = 0$ otherwise. Clearly, a homogeneous element $f s^i \in S$ ($f \in P$) belongs to the graded subalgebra R if and only if f is multi-homogeneous and $\partial(f) = 1^i$. In other words, $R_i = R \cap S_i = S_{1^i,i} = P_{1^i} s^i$.

Lemma 6.3. *Let $f s^l \in S$ with $f \in P$ a multi-homogeneous element and consider $f_{ij} s^i, g_j s^j, h_{jk} s^k \in S$ where $f_{ij}, g_j, h_{jk} \in P$ are multi-homogeneous elements such that $f s^l = \sum_{i+j+k=l} f_{ij} s^i g_j s^j h_{jk} s^k$. Then, from $f s^l \in R$ it follows that $f_{ij} s^i, g_j s^j, h_{jk} s^k \in R$, for all i, j, k.*

Proof. Clearly we have $f = \sum_{i+j+k=l} f_{ij} g_j^{s^i} h_{jk}^{s^{i+j}}$. Denote $\mu = \partial(f_{ij}), \nu = \partial(g_j^{s^i})$ and $\rho = \partial(h_{jk}^{s^{i+j}})$ and put $\alpha = \min\{k \mid \nu_k > 0\}$ and $\beta = \min\{k \mid \rho_k > 0\}$. By definition of the map σ, one has that $\alpha \geq i + 1$ and $\beta \geq i + j + 1$. If we assume $f s^l \in R$ that is $1^l = \partial(f) = \mu + \nu + \rho$, then necessarily $\mu = 1^i, \nu = i \cdot 1^j$ and $\rho = (i + j) \cdot 1^k$ and hence $\partial(f_{ij}) = 1^i, \partial(g_j) = 1^j, \partial(h_{jk}) = 1^k$. $\square$

Proposition 6.4. *Let I be a graded (two-sided) ideal of $R \subset S$ and let J be the* extension *of I to S that is J is the (multigraded) ideal generated by I in S. If G is a multi-homogeneous basis of J then $G \cap R$ is a (homogeneous) basis of I. In particular, the* contraction *$J \cap R$ is equal to I, that is there is a* bijective correspondence *between all graded ideals of R and their extensions to S.*

Proof. Consider $f s^l \in I \subset R$ ($f \in P$) a homogeneous element and let $G = \{g_j s^j\}$ with $g_j \in P$, g_j multi-homogeneous. Since f is multi-homogeneous and G is a basis of $J \supset I$, one has $f s^l = \sum_{i+j+k=l} f_{ij} s^i g_j s^j h_{jk} s^k$ with $f_{ij}, h_{jk} \in P$, f_{ij}, h_{jk} multi-homogeneous. From Lemma 6.3 it follows immediately that all elements $f_{ij} s^i, g_j s^j, h_{jk} s^k \in R$ that is $G \cap R$ is a basis of I. $\square$

Proposition 6.5. *Let $I \subset R$ be a graded ideal and let $J \subset S$ be its extension. If $G \subset J$ is a multi-homogeneous Gröbner basis of J then $G \cap R$ is a homogeneous Gröbner basis of I.*

Proof. If $fs^l = \sum_{i+j+k=l} f_{ij} s^i g_j s^j h_{jk} s^k$ is a Gröbner representation in S of a homogeneous element $fs^l \in I \subset J$ with respect to $G = \{g_j s^j\}$, then it is sufficient to use the same argument of Proposition 6.4 to obtain that fs^l has a Gröbner representation in R with respect to $G \cap R$. □

We obtain finally an algorithm to compute Gröbner bases of graded two-sided ideals of the subring $R \subset S$ which is isomorphic to the free associative algebra F by the map ι. Note that the considered monomial orderings on F are obtained as the restriction of monomial orderings on S to the monomial subalgebra R. By applying Proposition 6.5, the computation of homogeneous Gröbner bases in R is obtained as a slight modification of the algorithm SkewGBasis for the ideals of S. It is interesting to note that the latter procedure is in turn a variant of the Buchberger algorithm for modules over commutative polynomial rings. Thus, we may say that these computations in associative algebras are reduced to analogue ones over commutative rings via the notion of skew polynomial ring (see also Section 7). This reverses somehow the trivial fact that commutative algebras are just a subclass of the associative ones.

Algorithm 6.1 FreeGBasis2

Input: H, a homogeneous basis of a graded two-sided ideal $I \subset R$.
Output: G, a homogeneous Gröbner basis of I.
$G := H$;
$B := \{(f, g) \mid f, g \in G\}$;
while $B \neq \emptyset$ **do**
  choose $(f, g) \in B$;
  $B := B \setminus \{(f, g)\}$;
  for all $i, j \geq 0, i + j = \deg_s(f) - \deg_s(g)$ and $\mathrm{spoly}(f, s^i g s^j) \in R$ **do**
    $h := \mathrm{Reduce}(\mathrm{spoly}(f, s^i g s^j), \Sigma\, G\, \Sigma)$;
    if $h \neq 0$ **then**
      $B := B \cup \{(g, h), (h, g), (h, h) \mid g \in G\}$;
      $G := G \cup \{h\}$;
    end if;
  end for;
  for all $i, j \geq 0, j - i = \deg_s(f) - \deg_s(g)$ and $\mathrm{spoly}(fs^i, s^j g) \in R$ **do**
    $h := \mathrm{Reduce}(\mathrm{spoly}(fs^i, s^j g), \Sigma\, G\, \Sigma)$;
    if $h \neq 0$ **then**
      $B := B \cup \{(g, h), (h, g), (h, h) \mid g \in G\}$;
      $G := G \cup \{h\}$;
    end if;
  end for;
end while;
return G.

Proposition 6.6. *The algorithm* FreeGBasis2 *is correct.*

Proof. Since G is multi-homogeneous implies that $\Sigma\, G\, \Sigma$ is also multi-homogeneous, the procedure Reduce clearly preserves multi-homogeneity. Moreover, any element $f \in G$ ($f \notin H$) is obtained by reduction of a S-polynomial, say h. Owing to Proposition 6.5 we are interested only in the elements $f \in R$ and this holds if and only if $h \in R$. $\square$

Assume now that the graded ideal $I \subset R$ has a finite number of generators up to some degree $d > 0$. Note that the d-truncated algorithm FreeGBasis2 has termination provided by termination of SkewGBasis as stated in Proposition 4.7. This generalizes a well-known result about algorithmic solution of the word problem (membership problem) for finitely presented graded associative algebras.

7. Letterplace in P

As in Section 5, consider the P-linear map $\pi : S \to P$ such that $s^i \mapsto 1$, for all i. Note now that $\iota' = \pi\iota : F \to P$ is an injective K-linear map such that $x_{i_1} \cdots x_{i_d} \in \mathrm{Mon}(F) \mapsto x_{i_1}(1) \cdots x_{i_d}(d) \in \mathrm{Mon}(P)$. Recall that $F = \bigoplus_i F_i$ is a graded algebra with respect to total degree. Moreover, consider the weight map $\mathrm{w} : \mathrm{Mon}(P) \to \mathbb{N}$ such that $\mathrm{w}(x_i(j)) = j$ for all i,j and the corresponding grading $P = \bigoplus_i P_i$ defined by the monoid $(\mathbb{N}, \oplus)$. Then, we have that ι' is a homogeneous map and $\iota = \xi\iota'$ which is an algebra homomorphism.

Definition 7.1. *Let $I \subset F$ be a graded (two-sided) ideal. Denote by $I' \subset P$ the* w*-graded Σ-invariant ideal Σ-generated by $\iota'(I)$. In other words, if $G = \{\iota'(f) \mid f \in I_i, i \geq 0\}$ then I' is the ideal of P generated by $\Sigma \cdot G$. We call I' the* letterplace analogue *of I.*

Proposition 7.2. *Let $I \subset F$ be a graded ideal and $I' \subset P$ its letterplace analogue. Denote by $J = I'^S$ the skew analogue of I' and call J the* skew letterplace analogue *of I. We have that J is the extension to S of the ideal $\iota(I) \subset R$. Then, there is a* bijective correspondence *between all graded ideals of F and their (skew) letterplace analogues.*

Proof. Let J' be the extension of $\iota(I)$ to S. By definition J' is the ideal generated by the elements $\iota(f) = \iota'(f)s^i$, for all $f \in I_i$. Since I' is Σ-generated by the w-homogeneous elements $\iota'(f)$ of weight i, we conclude that $J = I'^S = J'$. Moreover, the bijective correspondence between graded two-sided ideals of F and their letterplace analogues in P is obtained by composing the bijections contained in Proposition 5.10 and Proposition 6.4. $\square$

The bijection between graded ideals of F and their letterplace analogues has been introduced in [17] and called "letterplace correspondence". The motivation of such name is essentially historical since the linear map ι' was first considered in [10, 6]. Note that in these articles the endomorphism σ and the algebra embedding ι were not introduced. The polynomial ring P was named there the "letterplace algebra" because in the monomial $\iota'(x_{i_1} \cdots x_{i_d}) = x_{i_1}(1) \cdots x_{i_d}(d)$ the indices $1, \ldots, d$ play the role of the "places" where the "letters" $x_{i_1}, \ldots, x_{i_d}$ occur in the word $x_{i_1} \cdots x_{i_d} \in \mathrm{Mon}(F)$.

Fix now a monomial ordering $\prec$ on the algebra S that is σ is compatible with the restriction of $\prec$ to $\mathrm{Mon}(P)$. By restricting $\prec$ to R one obtains a monomial ordering on F. Denote by V the image of the map ι' that is $V = \bigoplus_i V_i$ is a graded subspace of P where $V_i = P_{1^i} \subset P_i$. Note that V is a left R-module isomorphic to $R \approx F$. In fact, $V = \pi(R)$ and the restriction $\pi : R \to V$ has the restriction $\xi : V \to R$ as its inverse. In [17] one has the following result which is now a direct consequence of Proposition 5.17 and Proposition 6.5.

Proposition 7.3. *Let $I \subset F$ be a graded ideal and denote by $J \subset P$ its letterplace analogue. Then J is a multigraded (hence* w*-graded) Σ-invariant ideal of P. If G is a multi-homogeneous (hence* w*-homogeneous) Gröbner Σ-basis of J then $\iota'^{-1}(G \cap V)$ is a homogeneous Gröbner basis of I.*

From this result and algorithm SigmaGBasis one obtains the correctness of the following procedure which also has been introduced in [17].

Algorithm 7.1 FreeGBasis

Input: H, a homogeneous basis of a graded two-sided ideal $I \subset F$.
Output: G, a homogeneous Gröbner basis of I.
$G := \iota'(H)$;
$B := \{(f, g) \mid f, g \in G\}$;
while $B \neq \emptyset$ **do**
  choose $(f, g) \in B$;
  $B := B \setminus \{(f, g)\}$;
  for all $i \geq 0$ and $\mathrm{spoly}(f, s^i \cdot g) \in V$ **do**
    $h := \mathrm{Reduce}(\mathrm{spoly}(f, s^i \cdot g), \Sigma \cdot G)$;
    if $h \neq 0$ **then**
      $B := B \cup \{(g, h), (h, g), (h, h) \mid g \in G\}$;
      $G := G \cup \{h\}$;
    end if;
  end for;
end while;
return $\iota'^{-1}(G)$.

Assume finally that the graded ideal $I \subset F$ has a finite number of generators up to some degree $d > 0$. Note that the d-truncated algorithm FreeGBasis has now termination provided by Proposition 5.19.

8. Conclusions and future directions

From the previous sections we can conclude that, owing to the notion of Gröbner Σ-basis and the skew letterplace embedding ι, the theory of non-commutative Gröbner bases developed for $K\langle X\rangle$ using the concepts of overlappings, tips or obstructions [12, 21, 22] can be deduced from, unified to the classical Buchberger theory for commutative polynomial rings based on S-polynomials, at least in the graded case. From a practical point of view, one obtains the alternative algorithms FreeGBasis and FreeGBasis2 which are implementable in any computer algebra system providing commutative Gröbner bases. The feasibility of such methods has been already shown in [17] where an implementation in Singular has been compared with fastest implementations of the classical non-commutative algorithm.

Moreover, the general theory developed in this paper can be applied to any context where a monoid of endomorphisms Σ acts on the polynomial algebra $P = K[X]$ in a way which is compatible with Gröbner bases theory. We propose not only an abstract definition of what this may mean contributing to a current research trend (see for instance [8, 1, 3]), but also a method to transfer the related algorithms from P to the skew monoid ring $S = P * \Sigma$ when a suitable grading is given for P. This theory applies in particular to the shift operators $x_i \mapsto x_{i+1}$ and hence a stimulating field of applications is the rings of difference polynomials. In particular, we aim to extend the Gröbner Σ-bases theory to any finitely generated commutative monoid $\Sigma = \langle \sigma_1, \ldots, \sigma_r\rangle$ in order to cover partial difference ideals and to develop methods for the non-graded case by means of suitable (de)homogenization techniques. An effective implementation of all proposed algorithms will be clearly important to understand the actual practicability of the methods.

References

[1] Aschenbrenner, M.; Hillar, C.J., Finite generation of symmetric ideals. *Trans. Amer. Math. Soc.*, **359** (2007), no. 11, 5171–5192.

[2] Bergman, G. M., The diamond lemma for ring theory. *Adv. in Math.*, **29** (1978), no. 2, 178–218.

[3] Brouwer, A.E.; Draisma, J., Equivariant Gröbner bases and the Gaussian two-factor model, 2010. *Mathematics of Computation*, DOI:10.1090/S0025-5718-2010-02415-9.

[4] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: Singular 3-1-1 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2010).

[5] De Concini, C.; Eisenbud, D.; Procesi, C., Young diagrams and determinantal varieties. *Invent. Math.*, **56**, (1980), no. 2, 129–165.

[6] Doubilet, P.; Rota, G.-C.; Stein, J., On the foundations of combinatorial theory. IX. Combinatorial methods in invariant theory. *Studies in Appl. Math.*, **53** (1974), 185–216.

[7] Drensky, V., Free algebras and PI-algebras. *Graduate course in algebra*. Springer-Verlag Singapore, Singapore, 2000.

[8] Drensky, V.; La Scala, R., Gröbner bases of ideals invariant under endomorphisms. *J. Symbolic Comput.*, **41** (2006), no. 7, 835–846.

[9] Eisenbud, D., Commutative algebra with a view toward algebraic geometry. *Graduate Texts in Mathematics*, 150. Springer-Verlag, New York, 1995.

[10] Feynman, R.P., An operator calculus having applications in quantum electrodynamics. *Physical Rev. (2)*, **84**, (1951), 108–128.

[11] Giambruno, A.; Zaicev, M., Polynomial identities and asymptotic methods. *Mathematical Surveys and Monographs*, 122. American Mathematical Society, Providence, RI, 2005.

[12] Green, E.L., An introduction to noncommutative Gröbner bases. Computational algebra (Fairfax, VA, 1993), 167–190, *Lecture Notes in Pure and Appl. Math.*, 151, Dekker, New York, 1994.

[13] Green, E.L., Multiplicative bases, Gröbner bases, and right Gröbner bases. Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998). *J. Symbolic Comput.*, **29** (2000), no. 4-5, 601–623.

[14] Greuel, G.-M.; Pfister, G., A Singular introduction to commutative algebra. Second edition. Springer, Berlin, 2008.

[15] Higman, G., Ordering by divisibility in abstract algebras. *Proc. London Math. Soc. (3)*, **2**, (1952). 326–336.

[16] Lam, T.Y., A first course in noncommutative rings. *Graduate Texts in Mathematics*, 131. Springer-Verlag, New York, 2001.

[17] La Scala, R.; Levandovskyy, V., Letterplace ideals and non-commutative Gröbner bases. *J. Symbolic Comput.*, **44** (2009), no. 10, 1374–1393.

[18] Levin, A., Difference algebra. *Algebra and Applications*, 8. Springer, New York, 2008.

[19] Li, H., Noncommutative Gröbner bases and filtered-graded transfer. *Lecture Notes in Mathematics*, 1795. Springer-Verlag, Berlin, 2002.

[20] McConnell, J.C.; Robson, J.C., Noncommutative Noetherian rings. *Graduate Studies in Mathematics*, 30. American Mathematical Society, Providence, RI, 2001.

[21] Mora, F., Gröbner bases for noncommutative polynomial rings. Algebraic algorithms and error correcting codes (Grenoble, 1985), 353–362, *Lecture Notes in Comput. Sci.*, 229, Springer, Berlin, 1986.

[22] Ufnarovski, V.A., On the use of graphs for calculating the basis, growth and Hilbert series of associative algebras. (Russian) Mat. Sb. 180 (1989), no. 11, 1548–1560, 1584; translation in *Math. USSR-Sb.*, **68**, (1991), no. 2, 417–428.

[23] Weispfenning, V., Finite Gröbner bases in non-Noetherian skew polynomial rings. In: Wang, P.S. (Ed.), Proc. of the International Symposium on Symbolic and Algebraic Computation. ISSAC'92, ACM Press, 329–334.

* Dipartimento di Matematica, via Orabona 4, 70125 Bari, Italia
E-mail address: lascala@dm.uniba.it

** RWTH Aachen, Templergraben 64, 52062 Aachen, Germany
E-mail address: levandov@math.rwth-aachen.de