ELSEVIER

Theoretical Computer Science 244 (2000) 1–33

Theoretical Computer Science

www.elsevier.com/locate/tcs

Fundamental Study

Computational ideal theory in finitely generated extension rings

Joachim Apel

Fakultät fur Mathematik und Inform. Universität Leipzig, Augustusplatz 10–11, D-04109 Leipzig, Germany

Received 18 August 1998; revised 15 October 1999; accepted 29 February 2000

Abstract

Since Buchberger introduced the theory of Gröbner bases in 1965 it has become an important tool in constructive algebra and, nowadays, Buchberger's method is fundamental for many algorithms in the theory of polynomial ideals and algebraic geometry. Motivated by the results in polynomial rings a lot of possibilities to generalize the ideas to other types of rings have been investigated. The perhaps most general concept, though it does not cover all possible extensions, is the theory of graded structures due to Robbiano and Mora. But in order to obtain algorithmic solutions for the computation of Gröbner bases it needs additional computability assumptions. In this paper we introduce natural graded structures of finitely generated extension rings and present subclasses of such structures which allow uniform algorithmic solutions of the basic problems in the associated graded ring and, hence, of the computation of Gröbner bases with respect to the graded structure. Among the considered rings there are many of the known generalizations. But, in addition, a wide class of rings appears first time in the context of algorithmic Gröbner basis computations. Finally, we discuss which conditions could be changed in order to find further effective Gröbner structures and it will turn out that the most interesting constructive instances of graded structures are covered by our results.

MSC: F.2.2; F.u.1; I.1.2

Keywords: Computable algebraic structures; Algebraic algorithms; Groebner bases in graded structures

1. Introduction

A widely studied problem in general algebra and theoretical computer science is the decidability of congruence relations of algebraic structures modulo a set of equations. In many applications the algebraic structures are groups or semigroups. Here, we will

E-mail address: apel@mathematik.uni-leipzig.de (J. Apel).

0304-3975/00/$ - see front matter
PII: S0304-3975(00)00172-9

focus on the case of rings. Given a ring R and a set $E \subseteq R^2$ of equations it is enough to investigate the zero congruence modulo E because of the underlying abelian group structure of a ring R. Instead of the binary congruence relation $\equiv_E$ generated by E one investigates the unary relation $I \subseteq R$ consisting of all left-hand sides of congruences $a \equiv_E 0$. Such a set I is called an ideal of R and studying congruence relations in ring theory means studying ideal theory and the usual notation for the quotient structure $R/\equiv_E$ in ring theory is R/I.

Naively, an algebraic structure is called computable if equality of elements is decidable, all operations are computable functions, and all relations are decidable. A quotient of a computable algebraic structure modulo a congruence relation is computable iff the congruence relation is decidable. Hence, computability of residue class rings R/I of constructive rings R reduces to the decidability of the ideal membership problem of I. For given elements $f_1,\dots,f_k \in R$ one may ask for a solution $(h_1,\dots,h_k) \in R^k$ of the homogeneous linear equation $\sum_{i=1}^k h_i f_i = 0$. The solutions are called left syzygies of $f_1,\dots,f_k$, the solution space is a left R-module. In non-commutative rings R also the more general homogeneous linear equations $\sum_{j=1}^l g_{i_j} f_{i_j} g'_{i_j} = 0$ are of interest. The solutions live in a direct sum of tensor products $R \otimes R$. They are called two-sided syzygies and form a R-bimodule.

In various types of rings the fundamental ideal theoretical problems of the decision of ideal membership and the computation of syzygy modules could be solved in an algorithmic way using the so-called Gröbner bases. Among the more complex applications there are the computation of ideal operations, e.g. intersection or quotient, and the computation of related objects, e.g. Hilbert functions. So, the algorithmic computation of and division modulo Gröbner bases can be considered as the fundamental problems of computational ideal theory. During the last more than three decades Buchberger's algorithm became a central tool in constructive commutative algebra and algebraic geometry (cf. [1, 9, 10, 12]) and motivated by the achievements in polynomial rings many efforts have been spent in generalizations to other types of rings.

The concept of graded structures due to Robbiano [27] and Mora [23] provides an excellent frame for investigating Gröbner bases in very general situations. What remains to do in a concrete application is to verify a series of computability conditions which have to be fulfilled in order to obtain not only existential statements on Gröbner bases but also constructive results such as decidability of the ideal membership problem or the computability of finite generating sets of syzygy modules. The bottleneck of this approach is the verification and algorithmic solution of properties and problems in the associated graded ring (conditions (iii)–(v) in Definitions 2 and 3). A first approach to illustrate the boundaries of constructiveness in the frame of graded structures was presented in [4]. Starting from a graded structure $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in})$ sufficient conditions ensuring that $\mathfrak{R}$ is an effective Gröbner structure, i.e. that $\mathfrak{R}$ allows the algorithmic computation of Gröbner bases, were derived. The motivation to start from $\mathfrak{R}$ was to maintain as much as possible generality. But it proved to be a disadvantage that the class of rings covered by the results remains widely hidden. Therefore, in this paper we use an opposite approach. We start with a well-ordered monoid Γ and a ring R

obtained by adjunction of finitely many elements $X=\{X_1,\dots,X_n\}$ to a ground ring Q. Then we associate a natural graded structure $\mathfrak{R}$ to these objects and investigate its constructiveness in dependence on Q, Γ, and the defining relations of R. More precisely, our aim is to find classes of rings whose natural graded structures allow the reduction of large subproblems to the valuation monoid Γ and the ground ring Q in order to obtain uniform algorithmic solutions.

The constructive instances of graded structures corresponding to successful generalizations of Buchberger's method can be divided in two main directions. The first considers polynomial rings $R=Q[X]$ in finitely many variables $X=\{X_1,\dots,X_n\}$ with more general ground rings Q than only fields. For instance, there were investigated situations with principal ideal domains Q (cf. [16, 25]) or, even more general, commutative rings Q in which linear equations are solvable (cf. [1, 9, 21, 29, 31, 32]). R is a graded ring with respect to the commutative monoid freely generated by X in all these cases. The second direction of generalizations keeps Q a (skew) field but relaxes the property that R is a graded ring. Examples are enveloping algebras of Lie algebra [8], algebras of solvable type [17], G-algebras [2, 3], and solvable polynomial rings [18]. The constructive instances of natural graded structures investigated here include all the above types of rings but, in addition, also combinations of the two main directions are subsumed. Of course, the extensions which do not fit in the frame of graded structures, e.g. group rings (cf. [19, 20, 28]) and reduction rings (cf. [11, 30]), are not covered here.

The paper is organized as follows. We start with a short explanation of Gröbner bases in polynomial rings over a computable field. In Section 3 we present an introduction to the theory of graded structures. Then we define the notion of natural Γ-graded structures $\mathfrak{R}$ of extension rings R of Q generated by a set X and outline the proof of the effective Gröbner structure property in Sections 4 and 5. Section 6 considers necessary conditions Q and Γ have to satisfy in an effective left, right, or two-sided Gröbner structure $\mathfrak{R}$. The presentation of R by Gröbner bases in free extensions of Q by X is subject of Section 7. Sections 8 and 9 provide algorithmic solutions for problems in the associated graded ring G of $\mathfrak{R}$ which are fundamental for the computation of Gröbner bases. Assumptions ensuring ascending chain conditions for one- or two-sided ideals of G are considered in Section 10. Section 11 shows that the conditions introduced so far allow the algorithmic computation of left syzygy modules of homogeneous left ideals of the associated graded ring. In particular, this finishes the proof of the first main result of the paper which concerns effective left Gröbner structures and is summarized in Theorem 6. Section 12 deals with the two-sided case. Some effective left Gröbner structures $\mathfrak{R}$ allow the application of a generalized Kandri-Rody/Weispfenning closure technique (see [17]) in order to compute Gröbner bases of two-sided ideals (see Theorem 7). Theorem 8 generalizes a result of Mora who was the first presenting algebras in which Gröbner bases of two-sided ideals can be computed in an algorithmic way while, in general, one-sided ideals are even not finitely generated in these algebras (see [24]). The aim of Section 13 is to give an impression when a graded structure can be an effective Gröbner structure though it does not satisfy the assumptions of

Theorems 6–8. We close the paper by presenting examples of effective Gröbner structures in Section 14.

Finally, we remark that *ring* always stands for associative ring with unit element in this paper. In particular, also ring extensions are considered only in this class. Moreover, by the symbol $\mathbb{Z}$ we denote the ring of integers and by $\mathbb{N}$ the additive monoid of non-negative integers.

2. Basic idea of Gröbner bases

Let $\mathfrak{K}$ be a computable field, $R=\mathfrak{K}[X_1,\dots,X_n]$ the polynomial ring over $\mathfrak{K}$ in the set $X=\{X_1,\dots,X_n\}$ of indeterminates, $I\subseteq R$ an ideal of R, and $F=\{f_1,\dots,f_k\}$ a finite generating set of I. We are looking for an algorithm deciding $a\in I$? for any given $a\in R$. Having such an algorithm one can derive algorithms for the computation in the quotient ring R/I.

Following the theory of Euclidean rings we ask for a division algorithm which for arbitrary given $a\in R$ computes polynomials $h_1,\dots,h_k\in R$ and $b\in R$ such that

$$a=\sum_{i=1}^{k} h_i f_i + b. \tag{1}$$

In addition, we require that the remainder b is bounded by a in some sense [1] and that b is uniquely determined by the residue class $a+I$, i.e. for all $a,a'\in R$ satisfying $a-a'\in I$ the division algorithm has to produce the same b. Since $a\in I$ iff the remainder b of a is 0 the ideal membership problem of I is decidable if such an algorithm exists.

The polynomial ring R is $\mathbb{N}$-graded. Each non-zero polynomial has a degree and if two homogeneous non-zero polynomials, i.e. all monomials occurring in the polynomial are of the same degree, are multiplied then the product is again homogeneous and its degree is equal to the sum of the degrees of the factors. For simplicity, we call 0 homogenous of every degree. Each polynomial $a\in R$ has a unique representation $a=a_0+a_1+\cdots+a_d$, where d is the degree of a and a_i is homogeneous of degree i. If all elements of F are homogeneous then we can divide each homogeneous part a_i of a by F using linear algebra methods, namely Gauss elimination. Adding the homogeneous division formulas provides a representation (1) of a which satisfies our above conditions. Let us consider such a "level by level" method for non-homogeneous F. Denote the highest homogeneous part of f_j by $\overline{f_j}$. We start by dividing a_d modulo $\overline{f_1},\dots,\overline{f_k}$ and obtain a formula $a_d=\sum_{i=1}^{k} u_i\overline{f_i}+b_d$ with homogeneous polynomials u_i and b_d. Then we compute $a':=a-\sum_{i=1}^{k} u_i f_i - b_d$ which is zero or has a lower degree than a. By recursion we compute a formula $a'=\sum_{i=1}^{k} h_i' f_i + b'$ and finally obtain $a=\sum_{i=1}^{k}(u_i+h_i')f_i+b_d+b'$. The degree of $b:=b_d+b'$ is at most as high as the degree of a. But, unfortunately, b needs not to be the same for all polynomials from $a+I$. Let us illustrate this by a simple example. Let $a=x$, $f_1=x^2+x, f_2=x^2$. The

[1] In particular, for $a=0$ also b must be zero.

above algorithm yields $b = x$. But $a = f_1 - f_2 \in I$ and, hence, a should have the same remainder as 0, which is 0. It is easy to observe that extending F by the polynomial $f_3 = f_1 - f_2 = x$ will remove our problem. The following question remains: how to find the polynomials of I which should be added to F? The answer is that one has to look for linear dependencies $\sum_{i=1}^{k} u_i \overline{f_i} = 0$ between the highest homogeneous parts of the elements of F, here the u_i are homogeneous polynomials and all non-zero summands have the same degree. Recall, $(u_1, \ldots, u_k)$ is a homogeneous syzygy of the highest homogeneous parts of the elements of F. Each such syzygy s can be associated with an element $\mathrm{lift}(s) := \sum_{i=1}^{k} u_i f_i \in I$. If some of the elements $\mathrm{lift}(s)$ have non-zero remainder modulo F then we know that our "level by level" division algorithm does not work correctly for this generating set F. Adding all the non-zero remainders to F will repair these problems but other may still remain. Repeating this process until all remainders are zero eventually will produce a set F for which the "level by level" method produces for all $a \in R$ a representation (1) satisfying our conditions.

Note, the set R_d of all homogeneous polynomials of fixed degree d (including the zero-polynomial) is a finite-dimensional linear space and we have $\dim_{\mathfrak{K}}(R_d) = \binom{n+d-1}{n-1}$. By splitting the degree levels we can achieve that all linear spaces of homogeneous polynomials become one dimensional. We introduce a $\mathbb{N}^n$-grading with respect to an arbitrary admissible term order[2] $\prec$ on R by defining the generalized degree of the polynomial $a \in R \setminus \{0\}$ to be the exponent vector of the largest monomial appearing in a with non-zero coefficient. For degree compatible orders $\prec$ this refines the ordinary $\mathbb{N}$-grading of R. The above division algorithm will work also in the context of the $\mathbb{N}^n$-grading. But, now, homogeneous means monomial. This essentially simplifies the divisions inside the degree levels and the computation of homogeneous syzygies of the highest homogeneous parts of the elements of F. The price is a higher number of different degree levels which have to be considered during the algorithm. In the case of a $\mathbb{N}^n$-grading our algorithm is exactly Buchberger's well-known algorithm for the computation of Gröbner bases of polynomial ideals.

Let us summarize the above algorithms. The division problem of an inhomogeneous $a \in R$ modulo a finite inhomogeneous basis $F \subset I$ was solved as follows:

(1) Divide the highest homogeneous part of a by the highest homogeneous parts of F, lift the division formula to the inhomogeneous case by substituting a and F for their highest parts. As result of the lifting process one obtains a formula $a = \sum_{i=1}^{k} u_i f_i + (a' + a'')$, where $a' = 0$ or a' is homogeneous and has the same (generalized) degree as a and $a'' = 0$ or a'' is of smaller (generalized) degree than a.

[2] The monoid $\mathbb{N}^n$ is isomorphic to the multiplicative monoid $T(X)$ of power products in $X_1, \ldots, X_n$. Originally admissible term order (c.f. [9, 12]) stands for an order $\prec$ of $T(X)$ which is compatible with multiplication, i.e. $\forall u, v, w \in T(X)$: $u \prec v \Rightarrow wu \prec wv$, and satisfies $\forall u \in T(X) \setminus \{1\}$: $1 \prec u$. The admissible term orders are exactly the monoid well-orders of $T(X)$. In this sense the notion of admissible term orders can be generalized to arbitrary monoids.

(2) By recursion compute a division formula for a'' and substitute it in the above formula for a.

An arbitrary given finite basis $F \subset I$ can be completed to a Gröbner basis of I by the algorithm:

(1) Compute a homogeneous generating set B of the syzygy module of the highest homogeneous parts of F.
(2) Divide the elements $\mathrm{lift}(s) \in I$ associated to the syzygies $s \in B$ modulo F and add all non-zero remainders to F.
(3) Repeat the process until no more non-zero remainders occur.

The basic idea behind both methods can be characterized as transforming the original problem to a homogeneous problem, solving the (often much simpler) homogeneous problem, lifting the homogeneous solution back to the inhomogeneous case using simple calculations in the polynomial ring R yielding a new inhomogeneous problem of smaller degree, iterating these steps will eventually solve the input problem. In this paper we will apply the same method in the more general context that the graded ring in which the homogeneous calculations take place may differ from the ring the original problem comes from.

The objects involved in this method will be introduced in the next section on graded structures.

3. Graded structures

Let R be a ring with unit element and $(\Gamma, \prec)$ a well-ordered monoid. Let ε denote the unit element of Γ and note the well-known fact that ε is the minimal element of Γ with respect to $\prec$. Finally, let $\varphi : R\backslash\{0\} \to \Gamma$ be a Γ-pseudo valuation function, i.e. it satisfies

$$\begin{aligned}&\varphi(u) = \varepsilon,\\ &a + b \neq 0 \Rightarrow \varphi(a+b) \preccurlyeq \max(\varphi(a), \varphi(b)),\\ &ab \neq 0 \Rightarrow \varphi(ab) \preccurlyeq \varphi(a) \circ \varphi(b)\end{aligned}$$

for all invertible elements $u \in R$ and all non-zero elements $a, b \in R$. For each $\gamma \in \Gamma$ the set $\mathscr{F}_\gamma = \{a \mid \varphi(a) \preccurlyeq \gamma\} \cup \{0\}$ is an additive subgroup of R and it is easy to prove that the family $\mathfrak{F} = (\mathscr{F}_\gamma)_{\gamma \in \Gamma}$ is a filtration of R. For each $\gamma \in \Gamma$ we define the quotient $G_\gamma = \mathscr{F}_\gamma / \hat{\mathscr{F}}_\gamma$ of $\mathscr{F}_\gamma$ by its subgroup $\hat{\mathscr{F}}_\gamma = \{0\} \cup \bigcup_{\gamma' \prec \gamma} \mathscr{F}_{\gamma'}$. For $a \in \mathscr{F}_\gamma$ we introduce the denotation $[a]_{\hat{\mathscr{F}}_\gamma}$ for the residue class $a + \hat{\mathscr{F}}_\gamma \in G_\gamma$. The equation

$$\forall a, b \in R\backslash\{0\} : [a]_{\hat{\mathscr{F}}_{\varphi(a)}} [b]_{\hat{\mathscr{F}}_{\varphi(b)}} = [ab]_{\hat{\mathscr{F}}_{\varphi(a) \circ \varphi(b)}}$$

determines a multiplication which makes the direct sum $G = \bigoplus_{\gamma \in \Gamma} G_\gamma$ a Γ-graded ring with unit element $[1]_{\hat{\mathscr{F}}_\varepsilon}$. G with this multiplication is called the associated graded ring of the filtered structure $(R, \mathfrak{F})$. The elements $u \in G_\gamma$ are homogeneous of degree γ

(denotation $\deg(u)=\gamma$). R and G are connected via the function in : $R \rightarrow G$ assigning each element $a \in R$ its initial form $\text{in}(a)=[a]_{\hat{\mathscr{F}}_{\varphi(a)}}$ (by definition $\text{in}(0)=0$). Let $\hat{G}=\bigcup_{\gamma \in \Gamma} G_\gamma$ denote the set of all homogeneous elements of G and $\text{in}^* : \hat{G} \rightarrow R$ an arbitrary section of in, i.e. $\text{in}(\text{in}^*(u))=u$ for all homogeneous elements $u \in G$.

Let us illustrate the notion of graded structure by explaining the objects introduced above for a list of examples of rings well-investigated in the theory of Gröbner bases.

(I) Let $R=\mathfrak{K}[X_1,\ldots,X_n]$ be a polynomial ring and $\Gamma=\mathbb{N}$ the monoid of non-negative integers with the ordinary $<$-order. The function φ assigns the degree to each non-zero polynomial. Then the abelian group $\mathscr{F}_d$ consists of all polynomials of degree less or equal than d and $\hat{\mathscr{F}}_d$ is its subgroup of the polynomials of degree strictly less than d. The associated graded ring G is isomorphic to R and the direct summands G_d are the abelian groups of homogeneous polynomials of degree d. For $a \neq 0$ the initial form $\text{in}(a)$ is the highest homogeneous part of a in the ordinary sense. Since $G=R$ we can choose in^* the identity on the set $\hat{G}$ of all homogeneous polynomials.

(II) Now, consider $R=\mathfrak{K}[X_1,\ldots,X_n]$ with $\Gamma=\mathbb{N}^n$ and an arbitrary admissible term order $\prec$. The function φ assigns to the polynomial $a \neq 0$ the largest (w.r.t. $\prec$) exponent vector of a power product occurring in a with non-zero coefficient. $\mathscr{F}_{(i_1,\ldots,i_n)}$ ($\hat{\mathscr{F}}_{(i_1,\ldots,i_n)}$) consists of all polynomials containing only power products whose exponent vector is less or equal (strictly less) than $(i_1,\ldots,i_n)$ w.r.t. $\prec$. Again, $G=R$. But $G_{(i_1,\ldots,i_n)}$ consists of all products $\alpha X_1^{i_1}\cdots X_n^{i_n}$, where $\alpha \in \mathfrak{K}$. The function in assigns to each polynomial its leading monomial and in^* acts identically.

(III) Let $R=\mathfrak{K}\langle X_1,\ldots,X_n\rangle$ be the free non-commutative polynomial ring, $\Gamma=\langle X_1,\ldots,X_n\rangle$ the word semigroup freely generated by $X_1,\ldots,X_n$ and $\prec$ a monoid well-order[3] of Γ. The function φ assigns the largest word appearing with non-zero coefficient to $a \in R\setminus\{0\}$. G is isomorphic to R. $\text{in}(a)$ is the monomial with largest word appearing in a, in^* acts identically.

(IV) Let $R=\mathfrak{K}\langle X_1,\ldots,X_n\rangle/(X_iX_j-X_jX_i-[X_i,X_j])$ be an enveloping algebra of a Lie algebra, $\Gamma=\mathbb{N}^n$ with degree compatible admissible term order $\prec$. As linear space R is equal to the polynomial ring in the Example (II) of this list and we can define φ in the same way as there. Then also the filtration $\mathfrak{F}$ and the additive structure of the associated graded G are the same as in Example (II). Moreover, also the multiplication in G is this of the commutative polynomial ring. So, we meet a graded structure where R and G are different. The function in assigns to $a \neq 0$ its largest monomial. But while multiplication of two monomials in R, in general, does not produce a monomial multiplication of the initial forms of two elements of R yields always a monomial since the multiplication takes place in

[3] Examples for monoid well-orders $\prec$ of the free-word semigroup are the orders which first compare the words using an admissible term order by forgetting non-commutativity and subsequently break ties using a lexicographical order.

the commutative polynomial ring G. In most applications in^* is chosen in such a way that the monomial $u \in G$ and $\mathrm{in}^*(u) \in R$ "look the same". Note, however, that they are different objects.

(V) Example (IV) can be generalized straightforward to an arbitrary algebra of solvable type with defining relations $X_iX_j + c_{i,j}X_jX_i + p_{i,j}$, $1 \leqslant j < i \leqslant n$. The admissible term order $\prec$ has to satisfy the additional condition that any power product occurring in $p_{i,j}$ with non-zero coefficient is less than X_iX_j. Moreover, the coefficients $c_{i,j}$, $1 \leqslant j < i \leqslant n$, are non-zero elements of $\mathfrak{K}$ such that the "commutative looking" power products $X_1^{i_1} \cdots X_n^{i_n}$ of R are linearly independent over $\mathfrak{K}$, hence the set $\{X_1^{i_1} \cdots X_n^{i_n}: (i_1, \ldots, i_n) \in \mathbb{N}^n\}$ is a $\mathfrak{K}$-vector space basis of R. There is one interesting difference to the previous example. If some of the $c_{i,j}$ are different from -1 then the associated graded ring is no longer a commutative polynomial ring. In this case it may happen that the product of two power products of G is only a monomial, more precisely a multiple of the expected power product by a non-zero element of $\mathfrak{K}$.

(VI) Let $\mathfrak{K}$ be a field of characteristic different from 2 and Φ: $\mathfrak{K}^n \times \mathfrak{K}^n \to \mathfrak{K}$ a symmetric bilinear form. We consider the Clifford algebra $R = \mathfrak{K}\langle X_1, \ldots, X_n\rangle / (X_iX_j + X_jX_i - \Phi(X_i, X_j) : 1 \leqslant i, j \leqslant n)$ and the valuation monoid $\Gamma = \mathbb{N}^n$ with arbitrary admissible term order $\prec$. In difference to the previous Example (V), here, the elements $X_1^{i_1} \cdots X_n^{i_n}$ are linearly dependent, a $\mathfrak{K}$-basis of R is formed by all elements of the form $X_{i_1}X_{i_2} \cdots X_{i_r}$, where $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant n$. The function φ is defined in the usual way, i.e. it assigns to each $a \neq 0$ the largest exponent vector of monomials appearing in a. We have $\hat{\mathscr{F}}_{\exp(X_i^2)} = \mathscr{F}_{\exp(X_i^2)}$, $1 \leqslant i \leqslant n$, for the induced filtration $\mathfrak{F}$ and for this reason $\mathrm{in}(X_i)^2 = 0$. Hence, G contains zero divisors, e.g. the monomials $\mathrm{in}(X_i)$ are nilpotent. To the function in^* apply the same remarks as in Example (IV).

Now, we come to the definition of Gröbner bases in graded structures.

Definition 1. With the above notation we call $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in})$ a *graded structure*. Furthermore, a set $F \subset R$ is called a *Gröbner basis* with respect to $\mathfrak{R}$ of the left (right, two-sided) ideal I generated by F if $\mathrm{in}(F)$ and $\mathrm{in}(I)$ generate the same left (right, two-sided) ideal of G. If F is a Gröbner basis of I with respect to $\mathfrak{R}$ and no proper subset of F has this property then F is called a *minimal Gröbner basis* of I with respect to $\mathfrak{R}$.

If the graded structure $\mathfrak{R}$ is clear from the context we will call F simply a Gröbner basis of I. But sometimes if we consider more than one graded structure in parallel, then we will also write shortly $\mathfrak{R}$-Gröbner basis instead of Gröbner basis with respect to $\mathfrak{R}$.

Definition 2. A graded structure $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in})$ is called an *effective left* (*right*) *Gröbner structure* if the following conditions are satisfied:

(i) the rings R and G and the ordered monoid Γ are computable algebraic structures,

(ii) φ and in are computable functions, and there exists a computable section in^* of the initial mapping,
(iii) the membership problem of homogeneous left (right) ideals of G given by an arbitrary finite homogeneous generating set is decidable,
(iv) for any finite set $H \subset G$ of homogeneous elements there can be computed a finite homogeneous generating set of the left (right) syzygy module $\text{LSyz}(H)$ $(\Re\, Syz(H))$ of H, and
(v) G is a left (right) noetherian ring.

Before, we consider the two-sided case we will briefly discuss the syzygy problem of two-sided ideals. Let E denote the subring of G which is generated by the unit element $[1]_{\hat{\mathscr{F}}_\varepsilon}$. G is a left and a right E-module, so the tensor product $G \otimes_E G$ is a well-defined E-bimodule. In the following we consider $G \otimes_E G$ with its natural G-bimodule structure. Let $H = \{h_1, \ldots, h_k\} \subset G$ be a finite subset of G and $S_H : (G \otimes_E G)^k \to G$ denote the G-bimodule homomorphism defined by $S_H(\sum_{j=1}^m a_j e_{i_j} b_j) = \sum_{j=1}^m a_j h_{i_j} b_j$, where $1 \leqslant i_j \leqslant k$ and $a_j e_{i_j} b_j$ denotes the tensor $a_j \otimes b_j$ belonging to the i_jth copy of $G \otimes_E G$. For any H the kernel $\ker S_H$ forms a G-submodule of $(G \otimes_E G)^k$, the so-called *syzygy module* $\text{Syz}(H)$ of H. Even for noetherian rings G the G-bimodule $(G \otimes_E G)^k$ need not to be noetherian. Therefore, a straightforward generalization of condition (iv) would be to strong. Mora solved the problem in [23] by asking for the computability of a finite non-trivial homogeneous generating set of $\text{Syz}(H)$. A homogeneous syzygy $\sum_{j=1}^m a_j e_{i_j} b_j \in \text{Syz}(H)$ is called *trivial* if the element $\text{lift}_F(\sum_{j=1}^m a_j e_{i_j} b_j) = \sum_{j=1}^m \text{in}^*(a_j) f_{i_j} \text{in}^*(b_j)$ can be reduced to zero modulo F for any set $F = \{f_1, \ldots, f_k\} \subset R$ such that $\text{in}(f_i) = h_i$ $(i = 1, \ldots, k)$. If B together with the trivial syzygies of H generate the syzygy module $\text{Syz}(H)$ then B is called a *non-trivial generating set* of $\text{Syz}(H)$.

Definition 3. A graded structure $\Re = (R, \Gamma, \varphi, G, \text{in})$ is called an *effective two-sided Gröbner structure* if the following conditions hold:
(i) the rings R and G and the ordered monoid Γ are computable algebraic structures,
(ii) φ and in are computable functions, and there exists a computable section in^* of the initial mapping,
(iii) the membership problem of homogeneous two-sided ideals of G given by an arbitrary finite homogeneous generating set is decidable,
(iv) for any finite set $H \subset G$ of homogeneous elements a finite non-trivial homogeneous generating set of the syzygy module $\text{Syz}(H)$ can be computed, and
(v) G satisfies the ascending chain condition for two-sided ideals.

Let $A \subseteq G$ be an arbitrary subring generated by the initial forms $\text{in}(a)$ of elements a belonging to the center of R. Obviously, A is contained in the center of G. By $\text{Syz}_A(H)$ we denote the image of the syzygy module of H under the natural G-bimodule homomorphism $\tau : (G \otimes_E G)^k \to (G \otimes_A G)^k$. Since all syzygies belonging to the intersection $\ker \tau \cap \text{Syz}(H)$ are trivial the following criterion can be used for the verification of condition (iv): if $\text{Syz}_A(H)$ is finitely generated then $\text{Syz}(H)$ has a finite non-trivial generating set and for any generating set B of $\mathrm{Syz}_A(H)$ the set $\{b \mid \tau(b) \in B\}$ is non-trivial generating set of $\mathrm{Syz}(H)$.

Let $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in})$ be an effective left (right, two-sided) Gröbner structure. Then for any finite subset $F \subset R$ there can be computed a left (right, two-sided) Gröbner basis of the left (right, two-sided) ideal of R generated by F in an algorithmic way [23]. Given $\mathfrak{R}$ it remains to check that the conditions (i)–(v) are satisfied. The large generality of the concept of graded structures is its power but as soon as effectiveness is concerned it becomes also its main difficulty. At the level of Definitions 2 and 3 no restrictions apply to the algorithms solving conditions (iii) and particularly (iv). This is a motivation to look for subclasses of effective graded structures which have uniform algorithms for deciding membership problems and computing syzygy modules of homogeneous ideals of the associated graded ring.

4. Natural graded structures of extension rings

In this section we will present a class of graded structures which extends our list from Section 3. We consider a ring R with a finite minimal generating set $X = \{X_1, \ldots, X_n\}$ over some ground ring Q. For an arbitrary well-ordered monoid $(\Gamma, \prec)$ with a minimal generating set $Y = \{Y_1, \ldots, Y_n\}$ the condition

$$a \in \mathfrak{F}_\gamma :\Leftrightarrow a \text{ is a finite sum of terms } r_0 X_{i_1} r_1 \cdots X_{i_k} r_k,$$
$$\text{where } r_0, \ldots, r_k \in Q \text{ and } Y_{i_1} \circ \cdots \circ Y_{i_k} \preccurlyeq \gamma$$

defines a Γ-filtration $\mathfrak{F} = (\mathscr{F}_\gamma)_{\gamma \in \Gamma}$ of R. Note, the enumerations of the elements of the generating sets X and Y of R and Γ, respectively, are considered to be fixed. At this stage of construction the only relationship between the generators X_i and Y_i consists in the same index i. Note, in general, renumbering the sets will alter the filtration $\mathfrak{F}$ and the possibility of algorithmic Gröbner basis computations may depend on the chosen enumerations.

Definition 4. For R, $(\Gamma, \prec)$, and $\mathfrak{F}$ as above, the Γ-graded structure $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in})$ induced by the function

$$\varphi(a) := \min\{\gamma \in \Gamma \mid a \in \mathscr{F}_\gamma\}, \ a \in R \backslash \{0\}$$

will be called the *natural* Γ-graded structure of R.

There is a natural isomorphism between the subring $Q \subseteq R$ and the subring $G_\varepsilon \subseteq G$ formed by all homogeneous elements of degree ε, where ε denotes the unit element of Γ. In the following G_ε and Q will be identified. Then G is a left and a right Q-module.

Note, using the above construction that any extension ring of Q can be associated with a Γ-graded structure with respect to an arbitrary well-ordered monoid Γ. Of course, in this general context the above-defined graded structures are not very helpful in applications. In general, even the function φ is not computable.

In the remaining sections we will introduce further conditions which will ensure constructiveness. Until now, there is no connection between R and Γ except that we assumed that both have finite minimal generating sets of the same cardinality. [4] On the one hand, it would be much too restrictive to require that R is the monoid ring $Q\langle\Gamma\rangle$ of Γ with coefficients from Q. For instance, Examples (IV)–(VI) from Section 3 are not of this type. But on the other hand it is clear that pushing the problems to the associated graded ring G will be not useful if there is no connection between the multiplicative structures of R and of G at all. But the multiplicative structure of G is determined by Γ up to a large extent.

5. Outline of investigations

Before we start to investigate the effectiveness of natural graded structures $\mathfrak{R}$ we will sketch and motivate the necessary constructions.

First, we have to find a suitable representation of a ring R which is obtained by adjoining finitely many elements $X_1,\ldots,X_n$ to some ground ring Q, i.e. we have to describe the relations between the X_j and between the X_j and the elements of Q. For this purpose we will construct a free object $A=\langle Q,X\rangle_{\hat{Q}}$ and represent R as a quotient A/K. From the undecidability of the word problem for semigroups it follows that for K given by a finite generating set even equality in R needs not to be decidable. We will overcome this difficulty by the restriction that K has to be given by a finite Gröbner basis. So, first we need a theory of Gröbner bases in the free object A. Two suitable graded structures $\mathfrak{A}$ and $\mathfrak{A}_\Gamma$ of A can be found in the class of natural graded structures defined in Section 4. But before we construct these graded structures let us illustrate the method by means of an example.

The method of presenting R as a quotient of a free object appears already in Examples (IV)–(VI) presented in Section 3. Consider the defining relations $X_iX_j + c_{i,j}X_jX_i + p_{i,j}$, $1\leqslant j<i\leqslant n$, from Example (V). Then the quotient is an algebra of solvable type iff all $c_{i,j}$ are non-zero and the above elements are a Gröbner basis in the graded structure (III), where the free non-commutative monoid $\langle X_1,\ldots,X_n\rangle$ is ordered by $\prec$ such that $X_jX_i \prec X_iX_j$ for all $1\leqslant j<i\leqslant n$ and all words appearing in $p_{i,j}$ are less (w.r.t. $\prec$) than X_jX_i. Algebras of solvable type can be investigated also without using the free non-commutative polynomial ring (see [17]). But for Clifford algebras and the more general class of G-algebras (see [2]) the representation by a Gröbner basis in the free non-commutative polynomial ring is essential. Besides algorithms for the computation in R the Gröbner basis provides complete knowledge about the zero-divisors of the associated graded ring G and this knowledge is essential for

[4] Note, even the condition $|X|=|Y|$ could be dropped. But having in mind the aim of cyclic homogeneous modules of the associated graded ring the above restriction is natural. However, the condition does not yet ensure cyclic modules G_γ, e.g. if R is a free non-commutative polynomial ring $\mathfrak{K}\langle X\rangle$ and Γ is the free commutative monoid generated by Y then a homogeneous element of the associated graded ring is a linear combination of words consisting of the same letters with the same multiplicity.

computing syzygies in G. Note, that we generalized not only the ring but also the valuation monoid to a free object. The latter ensured that in our example the homogeneous modules of the associated graded ring are cyclic.

On the one hand, the non-commutative polynomial ring $Q\langle X\rangle$ would be too special for our investigations since the elements of Q do not need to commute with the generators X. On the other hand, the free object $\langle Q,X\rangle$ in the class of all extension rings of Q generated by $|X|$ elements is too general because the kernel of the canonical homomorphism from $\langle Q,X\rangle$ to R is not finitely generated in almost all interesting applications, e.g. consider once more the definition of an algebra of solvable type (see Example (V) in Section 3) but now as a quotient of $\langle \mathfrak{K},\{X_1,\dots,X_n\}\rangle$ instead of $\mathfrak{K}\langle X_1,\dots,X_n\rangle$. In this case there appear additional defining relations of the form $\alpha X_i - X_i\alpha$, where $\alpha\in\mathfrak{K}$.

A good compromise is to fix a subring $\hat{Q}\subseteq Q$ whose elements commute with all elements of the ring R and to consider the ring $A=\langle Q,X\rangle_{\hat{Q}}$ which is freely generated by X in the class of all extension rings of Q whose center contains $\hat{Q}$. At least the subring of Q which is generated by 1 is a suitable ring $\hat{Q}$ since all extension rings are assumed to have a unit element, too. In order to obtain a computable ring A the subring $\hat{Q}$ has to be chosen in such a way that Q is a computable $\hat{Q}$-module. Fix a monoid well-order $\prec_A$ of $\langle Y\rangle$ such that $\forall u,v\in\langle Y\rangle: v(u)\prec v(v)\Rightarrow u\prec_A v$, where $v:\langle Y\rangle\to\Gamma$ denotes the natural epimorphism acting identically on Y. Let $\mathfrak{A}=(A,\langle Y\rangle,\varphi_A,G_A,\mathrm{in}_A)$ be a natural graded structure according to Definition 3 (for the case $R=A$ and $(\Gamma,\prec)=(\langle Y\rangle,\prec_A)$). The ring A is computable. Moreover, for decidable $\prec_A$ also the associated graded ring G_A of $\mathfrak{A}$ is computable. In Section 7, we will introduce some restrictions on the ideals K we are interested in. At least for those ideals the $\mathfrak{A}$-Gröbner basis property is decidable. Moreover, if K has a finite $\mathfrak{A}$-Gröbner basis then the usual Gröbner basis completion method for graded structures eventually will have computed one. However, in general, no finite Gröbner basis of K need to exist as the following simple example shows. Let R be the G-algebra defined by the relations $\{yx-xy,zy-yz,zx-xz,xyz\}$, which indeed is simply a quotient of a commutative polynomial ring. The kernel K of the canonical homomorphism from $A=\mathfrak{K}\langle x,y,z\rangle$ to R contains the elements xy^kz, $k=1,2,\dots$, hence, any Gröbner basis of K with respect to the graded structure (III) is infinite. This motivation is enough to look for possibilities to relax the condition that R has to be presented by a Gröbner basis of K with respect to the natural $\langle Y\rangle$-graded structure $\mathfrak{A}$ of A. We introduce a second natural graded structure $\mathfrak{A}_\Gamma=(A,\Gamma,\varphi_\Gamma,G_\Gamma,\mathrm{in}_\Gamma)$ of the free object A. In difference to $\mathfrak{A}$, here, we use the same valuation monoid $(\Gamma,\prec)$ as in the graded structure $\mathfrak{R}$. It is well known that any Gröbner basis of an ideal $I\subseteq A$ with respect to $\mathfrak{A}$ is also a Gröbner basis of I with respect to $\mathfrak{A}_\Gamma$.[5]

The advantage of $\mathfrak{A}_\Gamma$ becomes clear when we look once more at our above example. In the case $\Gamma=\mathbb{N}^n$ the finite set $\{yx-xy,zy-yz,zx-xz,xyz\}$ consists of homogeneous elements with respect to a Γ-grading of $\mathfrak{K}\langle x,y,z\rangle$. Hence, it is a $\mathfrak{A}_\Gamma$-Gröbner basis of K. In Definition 5 we will introduce the notion of a Γ-truncation of a $\mathfrak{A}$-Gröbner

[5] In general, the opposite is wrong.

basis. Such Γ-truncations combine the advantage of simple calculations with respect to $\mathfrak{A}$ and the advantage of smaller Gröbner bases with respect to $\mathfrak{A}_\Gamma$.

In summary, our strategy is to present K by a Γ-truncation H_{trunc} of a Gröbner basis H with respect to $\mathfrak{A}$ and then to derive sufficient conditions for the natural graded structure $\mathfrak{R}$ to be an effective (left, right, two-sided) Gröbner structure in dependence on Q, Γ and H_{trunc}. The diagram

$$\begin{array}{lcccc}
\mathfrak{A} = (A, \langle Y\rangle, \varphi_A, G_A, \mathrm{in}_A) & : & A = \langle Q,X\rangle_{\hat{Q}} & (\langle Y\rangle, \prec_A) & \\
 & & \| & \downarrow \nu & \\
\mathfrak{A}_\Gamma = (A, \Gamma, \varphi_\Gamma, G_\Gamma, \mathrm{in}_\Gamma) & : & A = \langle Q,X\rangle_{\hat{Q}} & (\Gamma, \prec) & \qquad (2) \\
 & & \downarrow \iota & \| & \\
\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in}) & : & R = A/K & (\Gamma, \prec) &
\end{array}$$

displays the relations between the involved objects and structures.

6. Conditions on Q and Γ

In this section we ask for necessary conditions on Q and Γ in order to have a chance to obtain an effective Gröbner structure $\mathfrak{R}$ in the third row of diagram (2). If the natural graded structure $\mathfrak{R}$ is an effective left Gröbner structure then Q has to be a computable noetherian ring with decidable left ideal membership problem. Moreover, for any finite subset $H \subset Q$ a finite generating set of the left syzygy module $\mathrm{LSyz}(H)$ can be computed. To sketch a proof consider the extension left ideal $G \cdot I$ of the left ideal $I \subset Q$. G needs not to be a flat extension of Q, for instance, the left syzygy module of $G \cdot I$ is not necessarily generated by homogeneous left syzygies of degree ε. But taking into account that G is a graded ring the computability conditions carry over from G to Q. Analogous arguments can be applied in the right and two-sided case.

Assume that the natural graded structure $\mathfrak{R}$ of the monoid ring $R = Q\langle\Gamma\rangle$ is an effective left, right, and two-sided Gröbner structure. Then also Γ has to fulfill rather strong conditions. So, Γ must be a computable well-ordered monoid. Furthermore, it has to satisfy a generalization of Dickson's Lemma [13], i.e. for any infinite sequence $\gamma_1, \gamma_2, \ldots$ of elements of Γ there exist positive integers $i < j$ and $k < l$ such that γ_i is a left divisor of γ_j and γ_k is a right divisor of γ_l. In this case we call Γ a noetherian monoid which reflects the fact that ascending chains of left, right, or two-sided monoid ideals, respectively, will always stabilize.[6] Further, necessary conditions on Γ are that left, right, and two-sided divisibility of elements of Γ is decidable and that minimal common left, right, and two-sided multiples of finite subsets of Γ can be computed algorithmically. We remark, that the decidability of left or right divisibility is equivalent to the seemingly much harder condition, that the set of all decompositions into

[6] If the graded structure of $R = Q\langle\Gamma\rangle$ is only required to be an effective two-sided Gröbner structure then a weaker generalization of Dickson's Lemma providing only the ascending chain condition for two-sided ideals would be sufficient. But for simplicity, we consider only the strongest generalization which is suitable for all three types of ideals.

irreducible factors is finite and computable in an algorithmic way for all $\gamma \in \Gamma$. This is an easy consequence of the following facts. Any noetherian well-ordered monoid Γ satisfies the left and right cancellation law and any element $\gamma \neq \varepsilon$ of Γ has only a finite number of decompositions into irreducible factors. It follows that the minimal generating set X of Γ is uniquely determined, finite, and consists exactly of the irreducible elements of $\Gamma \setminus \{\varepsilon\}$.

7. Representation of R by Gröbner bases in free structures

For the rest of the paper we will restrict the class of considered graded structures $\mathfrak{R}$ by the condition that each quotient $G_\gamma = \mathscr{F}_\gamma / \hat{\mathscr{F}}_\gamma$, $\gamma \in \Gamma$, is either the zero module or generated by the element

$$\mathfrak{g}_\gamma := \mathrm{in}(X_{i_1} \cdots X_{i_k}), \text{ where } Y_{i_1} \cdots Y_{i_k} = \min_{\prec_A}\{u \in \langle Y \rangle \mid v(u) = \gamma\} \tag{3}$$

as a left and as a right Q-module. By definition let $\mathfrak{g}_\gamma := 0$ for all γ such that $G_\gamma = \{0\}$. Then we have

$$G = \bigoplus_{\gamma \in \Gamma} Q \cdot \mathfrak{g}_\gamma = \bigoplus_{\gamma \in \Gamma} \mathfrak{g}_\gamma \cdot Q. \tag{4}$$

All G_γ are cyclic left Q-modules and, hence, for each $\gamma \in \Gamma$ there exists a homomorphism $\sigma_\gamma : Q \to Q$ satisfying

$$\mathfrak{g}_\gamma a - \sigma_\gamma(a)\mathfrak{g}_\gamma = 0 \text{ for all } a \in Q. \tag{5}$$

A cyclic left Q-module M is determined by its *annihilating left ideal*

$$\mathrm{ann}_\mathrm{L}\, M = \{a \in Q \mid am = 0 \text{ for all } m \in M\}$$

up to isomorphism. We have $M \simeq Q/\mathrm{ann}_\mathrm{L}\, M$. An analogous statement holds for right Q-modules M and annihilating right ideals $\mathrm{ann}_\mathrm{R}\, M$. Both, left and right annihilators are even two-sided ideals of Q and for M being generated by the same element $\mathfrak{g}$ as a left and as a right Q-module it follows the ring isomorphism

$$Q/\mathrm{ann}_\mathrm{L}\, M \simeq Q/\mathrm{ann}_\mathrm{R}\, M. \tag{6}$$

Moreover,

$$a \in \mathrm{ann}_\mathrm{L}\, M \Leftrightarrow a\mathfrak{g} = 0, \quad a \in \mathrm{ann}_\mathrm{R}\, M \Leftrightarrow \mathfrak{g}a = 0.$$

We remark that the restriction to cyclic modules G_γ is typical but not necessary for Gröbner basis investigations. For instance, the main theorem on abelian groups can be applied successfully in many situations where the G_γ are of higher dimension. Mora and Möller investigated such situations in [22]. Also Hironaka's standard bases in power series rings refer to a grading with non-cyclic homogeneous summands (see [15]). [7]

[7] Note, Hironaka's grading is based on an order $\prec$ which is not well-founded. This leads to additional computability problems which were discussed in [5].

Pesch introduced a Gröbner theory in iterated Ore extensions (see [26]). Though, there is a natural translation of Pesch's method in the language of graded structures the result is not one of the known constructive instances. The direct summands G_γ of the associated graded ring are only cyclic as left Q-modules but higher dimensional as right Q-modules.

Now, we will investigate the structure of a Gröbner basis H of $K = \ker\iota$ with respect to $\mathfrak{A}$. According to Eq. (5) for all $\alpha \in Q$ and X_i in X the kernel $\ker\iota$ contains an element of the form

$$X_i\alpha - \sigma_{Y_i}(\alpha)X_i + p_{i,\alpha}, \tag{7}$$

where $p_{i,\alpha} = 0$ or $p_{i,\alpha} \in R$ with $v(\varphi_A(p_{i,\alpha})) \prec v(Y_i) = Y_i$.

Consider an arbitrary $t = Y_{i_1}\cdots Y_{i_k} \in \langle Y\rangle$ and let $Y_{j_1}\cdots Y_{j_l} = \min_{\prec_A}\{u \in \langle Y\rangle \mid v(u) = v(t)\}$. Then K contains an element

$$X_{i_1}\cdots X_{i_k} - \alpha_t X_{j_1}\cdots X_{j_l} + q_t, \tag{8}$$

where $\alpha_t \in Q$ and $q_t = 0$ or $v(\varphi_A(q_t)) \prec v(t)$. Furthermore, in the special case $l = k$ and $j_1 = i_1, \ldots, j_k = i_k$ the ideal K can contain elements

$$\beta_t X_{j_1}\cdots X_{j_l} + r_t, \tag{9}$$

where $\beta_t \in \mathrm{ann}_{\mathrm{L}} G_{v(t)}$ and $r_t = 0$ or $v(\varphi_A(r_t)) \prec v(t)$.

Since $Q \cap K = \{0\}$ there exists a minimal $\mathfrak{A}$-Gröbner basis H of K consisting only of elements of types (7)–(9). Recall, that any $\mathfrak{A}$-Gröbner basis of K is also a (possibly redundant) $\mathfrak{A}_\Gamma$-Gröbner basis of K. We define: [8]

Definition 5. A subset $H_{\mathrm{trunc}} \subseteq H$ of a minimal Gröbner basis H of K with respect to $\mathfrak{A}$ is called a *Γ-truncation* of H if H_{trunc} is a Gröbner basis of K with respect to $\mathfrak{A}_\Gamma$.

Note, that Γ-truncations of minimal $\mathfrak{A}$-Gröbner bases are $\mathfrak{A}_\Gamma$-Gröbner bases which have a particular structure. Given a finite Γ-truncated $\mathfrak{A}$-Gröbner basis H_{trunc} of K we can compute a finite set

$$D_t := \{h \in H' \mid \varphi_A(h) | t\}, \tag{10}$$

where H' denotes some minimal $\mathfrak{A}$-Gröbner basis of K, for an arbitrary given $t = Y_{i_1}\cdots Y_{i_k} \in \langle Y\rangle$.

More precisely, consider $t = Y_{i_1}\cdots Y_{i_k} \in \langle Y\rangle$ and let $\gamma := v(t) = Y_{i_1}\circ\cdots\circ Y_{i_k}$. We divide all products $X_{j_1}\cdots X_{j_m} g X_{p_1}\cdots X_{p_l}$, where $g \in H_{\mathrm{trunc}}$ and $Y_{j_1}\circ\cdots\circ Y_{j_m}\circ v(\varphi_A(g))\circ Y_{p_1}\circ\cdots\circ Y_{p_l} \mid \gamma$, by the set H_{trunc} with respect to the graded structure $\mathfrak{A}$. The elements of types (7) and (8) which are needed in D_t were already contained in H_{trunc}. Since

[8] In a previous version of this paper (see [6]) the notion of *truncated Gröbner basis* was defined in a very technical way without using the graded structure $\mathfrak{A}_\Gamma$. I am thankful to Teo Mora and the anonymous referees for pushing me to illustrate the notion. Thinking about explanations and illustrations of the old notion I discovered the equivalence to the much simpler notion presented here.

by definition H_{trunc} is a $\mathfrak{A}_\Gamma$-Gröbner basis we know that the $\mathfrak{A}_\Gamma$-initial form of each element $h \in K$ such that $\varphi_\Gamma(h)$ divides γ has a $\mathfrak{A}_\Gamma$-homogeneous representation in terms of the $\mathfrak{A}_\Gamma$-initial forms of the elements of H_{trunc}. Hence, each such h is a Q-linear combination of the products $X_{j_1} \cdots X_{j_m} g X_{p_1} \cdots X_{p_l}$ considered above. The initial form of an element h of type (9), where $\beta_t \neq 0$, is monomial in both graded rings G_A and G_Γ. The division of the products $X_{j_1} \cdots X_{j_m} g X_{p_1} \cdots X_{p_l}$ modulo H_{trunc} with respect to $\mathfrak{A}$ acts like Gauss elimination and produces all elements of type (9) belonging to some suitable set D_t.

Let us illustrate the idea behind the Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis H. The ordinary meaning of the truncation of H at $t \in \langle Y \rangle$ is the initial segment $H_t := \{h \in H \mid \varphi_A(h) \preccurlyeq_A t\}$. Such truncations proved to be very useful in the treatment of homogeneous ideals. It is well-known that the ideal membership problem of finitely generated homogeneous ideals of free non-commutative polynomial rings over a constructive field is decidable. The decision algorithm is based on the fact that, in spite of possibly infinite minimal Gröbner bases, one can compute a truncation of a minimal Gröbner basis at an arbitrary given degree.

In our situation the Γ-truncations H_{trunc} are often more practical than ordinary truncations H_t since the latter may be infinite for orders $\prec_A$ which are not degree compatible. Moreover, the possibility to compute a finite set D_t for an arbitrary $t \in \langle Y \rangle$ enables to decide the ideal membership problem of K in a similar way as by means of ordinary truncations in the homogeneous case.

Let us consider the structure of a minimal $\mathfrak{A}$-Gröbner basis in more detail. By $Y_\Gamma \subseteq \langle Y \rangle$ we denote the set of all words which are the minimal (with respect to $\prec_A$) element of an equivalence class of elements having the same image under v, in fact $Y_\Gamma \subseteq \langle Y \rangle$ is a set of canonical representants modulo the homomorphism v and identifying the canonical representants with the elements of Γ yields a set embedding of Γ in $\langle Y \rangle$. Obviously, a minimal $\mathfrak{A}$-Gröbner basis contains only such elements $h = X_{i_1} \cdots X_{i_k} - \alpha_t X_{j_1} \cdots X_{j_l} + q_t$ for which $\varphi_A(h) = Y_{i_1} \cdots Y_{i_k} \notin Y_\Gamma$ but $t \in Y_\Gamma$ for all proper subwords t of $\varphi_A(h)$. Hence, given any confluent term rewriting system which defines Γ as a quotient of the free monoid $\langle Y \rangle$, only the left-hand sides of the rewriting rules need to be considered as the possible highest term of $\mathfrak{A}$-Gröbner basis elements of type (8). In particular, if Γ is the free commutative monoid generated by Y then w.l.o.g. we can assume that all $\mathfrak{A}$-Gröbner basis elements of type (8) have the form $h = X_i X_j - \alpha_{i,j} X_j X_i + q_{i,j}$, where $1 \leqslant j < i \leqslant n$ and $q_{i,j} = 0$ or $\varphi_A(q_{i,j}) \prec_A Y_i Y_j$. Moreover, if $q_{i,j} \neq 0$ then it will follow $\varphi_\Gamma(q_{i,j}) \prec_\Gamma Y_i \circ Y_j = Y_j \circ Y_i$ by the properties of $\prec_A$. Similar arguments apply also to non-free commutative monoids Γ. But some of the $\alpha_{i,j}$ are zero in this case. Finally, if Γ is commutative and Q is a finitely generated $\hat{Q}$-module, let us say by $\{c_1, \ldots, c_r\}$, then H has a minimal $\mathfrak{A}$-Gröbner basis of the form

$$\begin{aligned}
&\underline{X_i c_j - \sigma_{Y_i}(c_j) X_i} + p_{i,j} \quad (1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant r),\\
&\underline{X_i X_j} - \alpha_{i,j} X_j X_i + q_{i,j} \quad (1 \leqslant j < i \leqslant n), \qquad (11)\\
&\underline{\beta_{(i_1,\ldots,i_l)} X_{i_1} \cdots X_{i_l}} + r_{(i_1,\ldots,i_l)} \quad (1 \leqslant i_1 \leqslant \cdots \leqslant i_l \leqslant n),
\end{aligned}$$

where the initial parts of the elements with respect to $\mathfrak{A}$ are underlined. Examples for $\mathfrak{A}$-Gröbner bases can be found in Section 14. The first example illustrates a case when all $\mathfrak{A}$-Gröbner bases are infinite but finite $\mathfrak{A}_\Gamma$-Gröbner bases and, hence, finite Γ-truncations of $\mathfrak{A}$-Gröbner bases exist.

In the following sections we will show how a finite Γ-truncation of a $\mathfrak{A}$-Gröbner basis H of K can be applied to the solution of some important algorithmic problems in $R = A/K$ and its associated graded ring with respect to the graded structure $\mathfrak{R}$. Together with a few more conditions these results will imply the computability of Gröbner bases with respect to $\mathfrak{R}$.

8. Computation of annihilating ideals of G_γ

Given a finite Γ-truncation H_{trunc} of a minimal $\mathfrak{A}$-Gröbner basis of K it is possible to compute a finite generating set of the annihilating left ideal $\mathrm{ann}_{\mathrm{L}} G_\gamma$ for any given $\gamma \in \Gamma$ in an algorithmic way.

Let $t = Y_{i_1} \cdots Y_{i_k} \in \langle Y \rangle$ be the (w.r.t. $\prec_A$) minimal word such that $v(t) = Y_{i_1} \circ \cdots \circ Y_{i_k} = \gamma$. Then we have

$$\alpha \in \mathrm{ann}_{\mathrm{L}} G_\gamma \Leftrightarrow \alpha X_{i_1} \cdots X_{i_k} \text{ is reducible (w.r.t. } \mathfrak{A}) \text{ modulo } H, \tag{12}$$

where H is an arbitrary Gröbner basis of $\ker \iota$ with respect to $\mathfrak{A}$.

Consider $h \in H$ with initial form $\mathrm{in}_A(h) = \beta_h X_{i_j} \cdots X_{i_m}$. Then the product $X_{i_1} \cdots X_{i_{j-1}} \mathrm{in}_A(h) X_{i_{m+1}} \cdots X_{i_k}$ is congruent to the monomial $\beta_{h,t} X_{i_1} \cdots X_{i_k} \in G_A$, where $\beta_{h,t} = \sigma_{Y_{i_1}}(\cdots (\sigma_{Y_{i_{j-1}}}(\beta_h)))$, modulo the two-sided ideal generated by the $\mathfrak{A}$-initial forms of the elements of H which belong to type (7). Obviously, $\beta_{h,t} \in \mathrm{ann}_{\mathrm{L}} G_\gamma$ for all so-constructed elements $\beta_{h,t} \in Q$. Furthermore, the right hand side of condition (12) means that for all $\alpha \in \mathrm{ann}_{\mathrm{L}} G_\gamma$ the homogeneous element $\alpha X_{i_1} \cdots X_{i_k} \in G_A$ must be a linear combination of homogeneous elements $X_{i_1} \cdots X_{i_{j-1}} \mathrm{in}_A(h) X_{i_{m+1}} \cdots X_{i_k}$, where h belongs to the set D_t defined in (10), $\varphi_A(h) = Y_{i_j} \cdots Y_{i_m}$, and $1 \leqslant j \leqslant m \leqslant k$. Hence, the annihilating left ideal $\mathrm{ann}_{\mathrm{L}} G_\gamma$ is generated by the above elements $\beta_{h,t}$. The set of all such $\beta_{h,t}$ is finite and can be constructed algorithmically since D_t can be computed from H_{trunc}.

For constructive G there are also computable homomorphisms $\widehat{\sigma_\gamma} : Q \to Q$ satisfying $a g_\gamma = g_\gamma \widehat{\sigma_\gamma}(a)$. This allows the transformation of the truncated Gröbner basis H_{trunc} in an equivalent system with all coefficients right of the products $X_{i_1} \cdots X_{i_k}$. Therefore, finite generating sets of the right annihilating ideals $\mathrm{ann}_{\mathrm{R}} G_\gamma$ can be computed in a similar way.

9. Ideal membership in the associated graded ring

Let $u_1, \ldots, u_k$, and v be non-zero homogeneous elements of the associated graded ring G of the natural graded structure $\mathfrak{R}$. Can we decide $v \in J$, where J is the left, respectively, two-sided, ideal generated by the elements $u_1, \ldots, u_k$? Our previous assumptions on Q, Γ, and K will turn out to be already sufficient to answer this question positively.

Let $\deg u_i = \gamma_i$ and $\deg v = \gamma$ denote the degrees of the homogeneous elements $u_1, \ldots, u_k$, and v. Then the elements can be assumed to be presented in the form $u_i = \alpha_i \mathfrak{g}_{\gamma_i}$, and $v = \beta \mathfrak{g}_\gamma$, where $\alpha_1, \ldots, \alpha_k, \beta \in Q$.

First consider left ideals J. The set $M = \{(\omega, i) \mid 1 \leqslant i \leqslant k \wedge \omega \circ \gamma_i = \gamma\}$ is finite and can be computed in an algorithmic way since divisibility in Γ is decidable. By constructiveness of G there is an algorithm transforming each product $\mathfrak{g}_\omega \alpha_i \mathfrak{g}_{\gamma_i}$, $(\omega, i) \in M$, in the form $\mathfrak{g}_\omega \alpha_i \mathfrak{g}_{\gamma_i} = \alpha'_{\omega,i} \mathfrak{g}_\gamma$, where $\alpha'_{\omega,i} \in Q$. Obviously,

$$
\begin{aligned}
v \in J &\Leftrightarrow \exists \beta_{\omega,i} \in Q \;:\; v = \sum_{(\omega,i) \in M} \beta_{\omega,i} \mathfrak{g}_\omega u_i \\
&\Leftrightarrow \beta \in Q \cdot (\alpha'_{\omega,i}) + \operatorname{ann}_{\mathrm{L}} G_\gamma. \qquad (13)
\end{aligned}
$$

Now, consider the two-sided ideal generated by $u_1, \ldots, u_k$. We can compute the set $M = \{(\omega, i, \omega') \mid 1 \leqslant i \leqslant k \wedge \omega \circ \gamma_i \circ \omega' = \gamma\}$, which is finite according to our assumptions. Applying similar arguments as in the left ideal case and taking into account that $\operatorname{ann}_{\mathrm{L}} G_\gamma$ is even two-sided it follows that

$$
\begin{aligned}
v \in J &\Leftrightarrow \exists \beta_{\omega,i,\omega';j}, \beta'_{\omega,i,\omega';j} \in Q \;:\; v = \sum_{(\omega,i,\omega') \in M} \sum_{j=1}^{m_{\omega,i,\omega'}} \beta_{\omega,i,\omega';j} \mathfrak{g}_\omega u_i \mathfrak{g}_{\omega'} \beta'_{\omega,i,\omega';j} \\
&\Leftrightarrow \beta \equiv \sum \beta_{\omega,i,\omega';j} \alpha'_{\omega,i,\omega'} \sigma_\gamma(\beta'_{\omega,i,\omega';j}) \bmod \operatorname{ann}_{\mathrm{L}} G_\gamma \\
&\Leftrightarrow \beta \in Q \cdot (\alpha'_{\omega,i,\omega'}) \cdot Q + \operatorname{ann}_{\mathrm{L}} G_\gamma, \qquad (14)
\end{aligned}
$$

where $\alpha'_{\omega,i,\omega'} \mathfrak{g}_\gamma = \mathfrak{g}_\omega u_i \mathfrak{g}_{\omega'}$.

In conclusion, we proved that the membership problem of a (left) homogeneous ideal of G can be reduced to the membership problem of a (left) ideal of Q. It is well-known that the decidability of $v \in J$? ensures the existence of an algorithm computing a representation of v in terms of $u_1, \ldots, u_k$ for any $v \in J$. However, due to its inefficiency, this general algorithm resulting from the theory is of no practical importance. Note, our above considerations prove not only decidability but provide also nice formulae transforming solutions of (13) and (14), respectively, in representations of v. Let $\delta_1, \ldots, \delta_m$ generate $\operatorname{ann}_{\mathrm{L}} G_\gamma$ as a left ideal. We have

$$
\begin{aligned}
&\beta = \sum_{(\omega,i) \in M} \beta_{\omega,i} \alpha'_{\omega,i} + \sum_{j=1}^{m} \mu_j \delta_j \\
&\Rightarrow v = \sum_{i=1}^{k} \left(\sum_{(\omega,i) \in M} \beta_{\omega,i} \mathfrak{g}_\omega \right) u_i
\end{aligned}
$$

and

$$\beta = \sum_{(\omega,i,\omega')\in M} \sum_{j=1}^{m_{\omega,i,\omega'}} \beta_{\omega,i,\omega';j}\alpha'_{\omega,i,\omega'}\beta'_{\omega,i,\omega';j} + \sum_{j=1}^{m} \mu_j \delta_{i_j} \mu'_j$$

$$\Rightarrow v = \sum_{(\omega,i,\omega')\in M} \sum_{j=1}^{m_{\omega,i,\omega'}} (\beta_{\omega,i,\omega';j}\mathfrak{g}_\omega) u_i (\mathfrak{g}_{\omega'}\widehat{\sigma}_\gamma(\beta'_{\omega,i,\omega';j})).$$

Hence, under some obvious conditions on the efficiency of calculations in Q, Γ, and G we obtain also efficient algorithms for the computation of representations of v in terms of $u_1,\dots,u_k$.

10. The noetherian property of G

Until now our conditions on Q, Γ, and K influenced mainly the Q-module structure but there are still to many freedoms in the ring structure of R and G. In particular, we have not yet enough control about the zero divisors of G.

Consider, for instance, the following extremal case. Let Γ be the free commutative monoid generated by Y and assume that the elements of Q commute with the elements of X, hence, $A = Q\langle X\rangle$ in diagram (2). Moreover, let $X_iX_j \in K$ for all $1 \leqslant j < i \leqslant n$ and K contain no element of type (9). Then G is non-noetherian and contains zero-divisors. For instance, the product uv of two monomials $u, v \in G$ is zero, whenever v contains a variable of smaller index than the highest index of variables contained in u. In particular, $\mathrm{in}(X_i)\mathrm{in}(X_j) = 0$ for all $1 \leqslant j < i \leqslant n$. The two-sided ideal of G generated by the homogeneous elements $\mathrm{in}(X_1X_2^kX_3)$, $k = 0, 1, \dots$, is not finitely generated, hence, G does not satisfy any ascending chain condition for one- or two-sided ideals.

In general, serious problems can appear if $\ker\iota$ contains elements of type (8) whose coefficient α_t is not invertible modulo $\mathrm{ann}_{\mathrm{L}}\, G_{v(t)}$. Such kernel elements can, but need not, cause a non-noetherian associated graded ring G.

The condition

$$\forall \gamma, \omega \in \Gamma : G_\gamma G_\omega = G_{\gamma\circ\omega} \tag{15}$$

is equivalent to the property that for any $t = Y_{i_1}\cdots Y_{i_k} \in \langle Y\rangle$ there exists $X_{i_1}\cdots X_{i_k} - \alpha_t X_{j_1}\cdots X_{j_l} + q_t \in \ker\iota$ of type (8) such that α_t is a unit modulo $\mathrm{ann}_{\mathrm{L}}\, G_{v(t)}$. Note, we call $\alpha \in Q$ a unit (or an invertible element) modulo the two-sided ideal $I \subseteq Q$ iff there exists $\alpha' \in Q$ such that $\alpha\alpha' - 1 \in I$ and $\alpha'\alpha - 1 \in I$. In particular, even 0 is a unit modulo $I = Q$ according to this definition.

If Q and Γ are noetherian and G satisfies condition (15) then the associated graded ring G is left and right noetherian. We show that any infinite sequence of non-zero homogeneous elements $u_1 = \mathfrak{g}_{\gamma_1}\alpha_1, u_2 = \mathfrak{g}_{\gamma_2}\alpha_2, \dots$ of G contains $u_l \in G(u_1,\dots,u_{l-1})$. Since Γ is noetherian there exists an infinite subsequence $u_{i_1}, u_{i_2}, \dots$ such that the degree of u_{i_k} is a right multiple of the degree of u_{i_j} for all $j < k$. Moreover, by condition

(15) for all $j<k$ it follows the existence of a homogeneous element $v_{j,k}$ such that $\mathfrak{g}_{\gamma_{i_k}} = v_{j,k}\mathfrak{g}_{\gamma_{i_j}}$. Furthermore, since Q is noetherian it follows the existence of an index $l>1$ such that α_{i_l} belongs to the left ideal of Q generated by the elements $\alpha_{i_1},\ldots,\alpha_{i_{l-1}}$. Consequently, there exist $\beta_1,\ldots,\beta_{l-1}\in Q$ such that $u_{i_l}=\mathfrak{g}_{\gamma_{i_l}}\alpha_{i_l}=\sum_{r=1}^{l-1} v_{r,l}\mathfrak{g}_{\gamma_{i_r}}\beta_r\alpha_{i_r}=\sum_{r=1}^{l-1} v_{r,l}\hat{\sigma}_{\gamma_{i_r}}(\beta_r)\mathfrak{g}_{\gamma_{i_r}}\alpha_{i_r}=\sum_{r=1}^{l-1}(v_{r,l}\hat{\sigma}_{\gamma_{i_r}}(\beta_r))u_{i_r}$. Hence, u_{i_l} belongs to the left ideal of G generated by $u_1,\ldots,u_{i_{l-1}}$ and it follows that G is a left noetherian ring. Starting with representations $u_i=c_i'\mathfrak{g}_{\gamma_i}$ we can prove in the same way that G is right noetherian and, hence, noetherian.

Next we change condition (15) in such a way that G still satisfies the ascending chain condition for two-sided but not longer necessarily for left or right ideals. Instead of (15) we assume now that the elements of Q commute with the elements of X and that for all $\omega\in\Gamma$ and divisors $\gamma\in\Gamma$ there exists a decomposition $\gamma'\circ\gamma\circ\gamma''=\omega$ such that

$$G_{\rho'}G_{\rho}G_{\rho''} = G_{\rho'\circ\rho\circ\rho''} \tag{16}$$

for all divisor triples $\rho'|\gamma'$, $\rho|\gamma$, $\rho''|\gamma''$. We will show that any infinite sequence $u_1=\mathfrak{g}_{\gamma_1}\alpha_1, u_2=\mathfrak{g}_{\gamma_2}\alpha_2,\ldots$ of homogeneous elements of G contains an element $u_k\in G(u_1,\ldots,u_{k-1})G$. Since Γ is noetherian it is sufficient to prove the assertion for sequences satisfying $\gamma_i\,|\,\gamma_j$ for all $i<j$. Since Q is noetherian there exists k such that $\alpha_k\in Q(\alpha_1,\ldots,\alpha_{k-1})Q$. For all $i<k$ there exist $\gamma_i',\gamma_i''\in\Gamma$ and $\beta_i\in Q$ such that $\beta_i\mathfrak{g}_{\gamma_i'}u_i\mathfrak{g}_{\gamma_i''}=\mathfrak{g}_{\gamma_k}\alpha_i$ according to the above assumptions. Hence, $u_k\in G(u_1,\ldots,u_{k-1})G$ and the ascending chain condition for two-sided ideals of G will follow.

Given a Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis of K condition (15) could be verified using a simple criterion checking whether the coefficients α_t appearing in the elements of type (8) are invertible modulo $\mathrm{ann}_{\mathrm{L}}G_{v(t)}$. When Γ is commutative and $G_{Y_{i_1}\circ Y_{i_2}\circ\cdots\circ Y_{i_k}}=G_{Y_{i_1}}G_{Y_{i_2}}\cdots G_{Y_{i_k}}$ for all $1\leqslant i_1\leqslant\cdots\leqslant i_k\leqslant n$[9] then a similar criterion allows the verification of condition (16). For each pair (i,j) such that $1\leqslant j<i\leqslant n$ the ideal K contains an element $X_iX_j-\alpha_{i,j}X_jX_i+q_{i,j}$ of type (8) and it is obvious how to construct these elements from an arbitrary Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis of K. Condition (16) holds iff for each $1\leqslant j\leqslant n$ we have at least one of the following two properties: (i) $\alpha_{i,j}$ is invertible modulo $\mathrm{ann}_{\mathrm{L}}G_{Y_j\circ Y_i}$ for all $j<i\leqslant n$ or (ii) $\alpha_{j,i}$ is invertible modulo $\mathrm{ann}_{\mathrm{L}}G_{Y_i\circ Y_j}$ for all $1\leqslant i<j$. Let $\gamma|\omega$, an example of a suitable decomposition $\omega=\gamma'\circ\gamma\circ\gamma''$ can be obtained by gathering all variables of the quotient ω/γ whose index j satisfies condition (ii) in γ' and the rest in γ''. Now, let us consider the opposite direction, i.e. for some $1\leqslant j\leqslant n$ neither condition (i) nor (ii) holds. Then there exist $i<j$ and $i'>j$ such that $\alpha_{j,i}$ and $\alpha_{i',j}$ are not invertible modulo the corresponding annihilating left ideals and for $\omega=Y_i\circ Y_j\circ Y_{i'}$ and $\gamma=Y_i\circ Y_{i'}$ no decomposition fulfills condition (16).

[9] Note, the most important case covered by these conditions is when Γ is the commutative monoid freely generated by Y and the order $t\prec_A s :\Leftrightarrow v(t)\prec v(s)\vee(v(t)=v(s)\wedge t<_1 s)$, where $<_1$ denotes the lexicographical order extending $Y_1<_1Y_2<_1\ldots<_1Y_n$, is used in the construction of $\mathfrak{A}$.

We remark, if Q is a field then condition (16) is equivalent to the assumption that for all ω and $\gamma|\omega$ there exist γ' and γ'' such that $\gamma'\circ\gamma\circ\gamma''=\omega$ and $G_{\gamma'}G_{\gamma}G_{\gamma''}=G_{\omega}$. But already for $Q=\mathbb{Z}$ the above condition is weaker than condition (16). For instance, consider $R=\mathbb{Z}\langle X_1,X_2,X_3\rangle/(X_2X_1-2X_1X_2,X_3X_2,X_3X_1,3X_1X_2X_3)$ and Γ the free commutative monoid generated by $\{Y_1,Y_2,Y_3\}$. There we have $G_{Y_2}G_{Y_1}G_{Y_3}=G_{Y_1Y_2Y_3}=\mathbb{Z}\cdot(X_1X_2X_3)\simeq\mathbb{Z}/3\mathbb{Z}$ in spite of $G_{Y_2}G_{Y_1}=\mathbb{Z}\cdot(2X_1X_2)\subsetneq G_{Y_1Y_2}=\mathbb{Z}\cdot(X_1X_2)$. Note, only the weaker condition had to be used in order to prove the noetherian property. However, the full strength of condition (16) will be required for the syzygy computation in the proof of Theorem 8.

11. Effective one-sided Gröbner structures

In this section, we assume that the associated graded ring G of $\mathfrak{R}$ satisfies the conditions (4) and (15). In order to prove that $\mathfrak{R}$ is an effective left Gröbner structure it remains to show that left syzygy modules of homogeneous ideals of G are computable. Our first considerations concern the degrees of the left syzygies which have to be contained in a homogeneous generating set of $\mathrm{LSyz}(U)$, where U is a finite set of homogeneous elements of G. Of course, the minimal common multiples of the degrees of the elements of U are of interest. But in addition, a zero relation may arise if a non-zero homogeneous combination of U is multiplied by a homogeneous element such that the coefficient of the product annihilates the direct summand of G belonging to the degree of the product. In order to characterize such situations we study the sets

$$\Gamma_{\gamma}=\{\omega\in\Gamma\mid G_{\gamma}\not\simeq G_{\omega\circ\gamma}\}. \tag{17}$$

As an immediate consequence of condition (15) we obtain that the product $\mathfrak{g}_{\omega}\mathfrak{g}_{\gamma}$ generates $G_{\omega\circ\gamma}$ as left and as right Q-module for all $\omega,\gamma\in\Gamma$. In particular, $\mathfrak{g}_{\omega}\mathfrak{g}_{\gamma}\alpha=0$ iff $\alpha\in\mathrm{ann}_{\mathrm{R}}G_{\omega\circ\gamma}$ and, hence, $\mathrm{ann}_{\mathrm{R}}G_{\gamma}\subseteq\mathrm{ann}_{\mathrm{R}}G_{\omega\circ\gamma}$. Consequently, the quotient ring $Q/\mathrm{ann}_{\mathrm{R}}G_{\omega\circ\gamma}$ is a homomorphic image of the quotient ring $Q/\mathrm{ann}_{\mathrm{R}}G_{\gamma}$ and the condition $\omega\notin\Gamma_{\gamma}$ is equivalent to $\mathrm{ann}_{\mathrm{R}}G_{\gamma}=\mathrm{ann}_{\mathrm{R}}G_{\omega\circ\gamma}$. Moreover, for arbitrary $\gamma,\omega,\omega'\in\Gamma$ there is a sequence

$$G_{\gamma}\simeq Q/\mathrm{ann}_{\mathrm{R}}G_{\gamma}\xrightarrow{\rho_{\omega,\gamma}}Q/\mathrm{ann}_{\mathrm{R}}G_{\omega\circ\gamma}\xrightarrow{\rho_{\omega',\omega\circ\gamma}}Q/\mathrm{ann}_{\mathrm{R}}G_{\omega'\circ\omega\circ\gamma}\simeq G_{\omega'\circ\omega\circ\gamma}$$

of epimorphisms. If $\rho_{\omega,\gamma}$ is not injective then also the composition of $\rho_{\omega,\gamma}$ and $\rho_{\omega',\omega\circ\gamma}$ is surjective but not injective. Since Q is noetherian the existence of a non-injective epimorphism implies that the rings are not isomorphic. Hence, with $\omega\in\Gamma_{\gamma}$ the set Γ_{γ} contains also the multiples $\omega'\circ\omega$ for all $\omega'\in\Gamma$.

In summary, for all $\gamma\in\Gamma$ the set Γ_{γ} is either empty or a left monoid ideal of Γ. Given a finite Γ-truncation H_{trunc} of a minimal $\mathfrak{A}$-Gröbner basis of K there is an obvious algorithm for the computation of a finite generating set[10] Δ_{γ} of Γ_{γ} for an arbitrary given $\gamma\in\Gamma$. Roughly, the idea behind is to extract a generating set Δ_{γ} from

[10] Formally, $\Delta_{\gamma}=\emptyset$ is considered as generating set of $\Gamma_{\gamma}=\emptyset$.

the set of all elements $\omega \in \Gamma$ for which $\omega \circ \gamma$ is a minimal common multiple of γ and the elements of some subset of $\{v(\varphi_A(h)) \mid h \in H_{\text{trunc}}\}$.

This can be applied to the algorithmic computation of the left syzygy module $\text{LSyz}(U)$ for an arbitrary finite set U of homogeneous non-zero elements of G. We define recursively $\Omega(U)_{i+1} = \{\gamma' \circ \gamma \mid \gamma \in \Omega(U)_i \wedge \gamma' \in \Delta_\gamma\}$, where the initial value $\Omega(U)_0 \subseteq \Gamma$ is the set of all minimal common right multiples of the degrees of elements of U. Each set $\Omega(U)_i$ is finite and can be computed algorithmically. If $\Omega(U)_i = \emptyset$ then $\Omega(U)_j = \emptyset$ for all $j > i$. By the properties of Q there cannot exist an infinite sequence $Q/\text{ann}_{\text{L}} G_{\gamma_0} \to Q/\text{ann}_{\text{L}} G_{\gamma_1} \to \cdots$ of non-injective ring epimorphisms. Hence, there exists a positive integer i_0 such that $\Omega(U)_{i_0} = \emptyset$ and, therefore, $\Omega(U) = \bigcup_{i=1}^{\infty} \Omega(U)_i = \bigcup_{i=1}^{i_0-1} \Omega(U)_i$ is finite and can be computed algorithmically. For arbitrary given $\gamma \in \Omega(U)$ there can be computed a finite generating set of the left syzygy module of $\{\delta + \text{ann}_{\text{L}} G_\gamma \mid \exists u \in U \exists \omega \in \Gamma\colon\ \mathfrak{g}_\omega u = \delta \mathfrak{g}_\gamma\} \subset Q/\text{ann}_{\text{L}} G_\gamma$ according to the properties of Q. These generating left syzygies can be lifted to homogeneous left syzygies of degree γ of U by multiplying each of their components from the right by the corresponding element $\mathfrak{g}_\omega$. Any homogeneous left syzygy of degree γ of U is contained in the left G-module generated by the set B_γ formed by the lifted left syzygies. Next, we show that any homogeneous left syzygy $s = \sum_{u \in U} h_u e_u$ of U, whose degree is a common right multiple of the degrees of all elements of U, belongs to the left G-module generated by the union $B(U) = \bigcup_{\gamma \in \Omega(U)} B_\gamma$. Let γ be a maximal right divisor of $\deg s$ which is contained in $\Omega(U)$ and $\omega \in \Gamma$ be such that $\omega \circ \gamma = \deg s$. According to condition (15) there exist homogeneous elements v_u such that $\mathfrak{g}_\omega v_u = h_u$ and, hence, s can be written in the form $s = \mathfrak{g}_\omega \sum_{u \in U} v_u e_u$. $\sum_{u \in U} v_u u$ is a homogeneous element of G of degree γ and, therefore, can be written in the form $\mathfrak{g}_\gamma d$, where $d \in Q$. Furthermore, $\mathfrak{g}_\omega \mathfrak{g}_\gamma d = 0$ since s is a left syzygy of U. Consequently, $d \in \text{ann}_{\text{R}} G_{\deg s} \supseteq \text{ann}_{\text{R}} G_\gamma$. By definition of $\Omega(U)$ the inclusion is even equality and, therefore, s is a multiple of a homogeneous left syzygy of U which has a degree contained in $\Omega(U)$.

In conclusion, the set $B(U) \cup \bigcup_{U' \subset U} \text{LSyz}(U')$, where $B(U) = \bigcup_{\gamma \in \Omega(U)} B_\gamma$, generates $\text{LSyz}(U)$ and induction on the number of elements of U yields that a finite homogeneous generating set of $\text{LSyz}(U)$ can be constructed in an algorithmic way.

Theorem 6. *Let Q be a computable noetherian ring with decidable ideal membership and solvable syzygy problem for left, right, and two-sided ideals, and $\hat{Q}$ a subring of the center of Q such that Q is a computable $\hat{Q}$-module. Furthermore, let Γ be a computable well-ordered monoid which is noetherian and allows algorithmic computation of minimal common multiples and factorial decompositions. Finally, let $R = \langle Q, X \rangle_{\hat{Q}}/K$ be given by a finite Γ-truncation H_{trunc} of a minimal $\mathfrak{A}$-Gröbner basis of the two-sided ideal K and let the associated graded ring G belonging to the natural graded structure $\mathfrak{R} = (R, \Gamma, \varphi, G, \text{in})$ satisfy conditions* (4) *and* (15).

Then $\mathfrak{R}$ is an effective left Gröbner structure.

Proof. Conditions (i)–(v) of Definition 2 have been verified already. □

Analogous considerations prove that any graded structure $\mathfrak{R}$ fulfilling the assumptions of the above theorem is also an effective right Gröbner structure. However, the assumptions could be slightly relaxed by assuming only the conditions on Q and Γ which refer to left (right) ideals. Among these marginal cases there are graded structures $\mathfrak{R}$ which are only an effective left (right) but not an effective right (left) Gröbner structure. For computable fields $\mathfrak{K}$ the graded structures (II), (IV), (V) and (VI) presented in Section 3 fulfill the assumptions of the above theorem. Besides the explicitly mentioned examples of enveloping algebras of Lie algebras and Clifford algebras also the classical examples of Weyl algebras and exterior algebras are covered by this list. In the next section, the two-sided case will be investigated and all the examples listed so far will satisfy also the stronger assumptions of Theorem 7. An example where only Theorem 6 for one-sided Gröbner structures is applicable [11] is the Hecke algebra $\mathscr{H}_r(q) = \mathbb{C}\langle X_1, \ldots, X_{r-1}\rangle / K$, where q is a non-zero complex number, $r \geqslant 2$ an integer, and K the two-sided ideal generated by the elements

$$\begin{aligned} &X_iX_{i+1}X_i - X_{i+1}X_iX_{i+1}, \quad i = 1, \ldots, r-2, \\ &X_iX_j - X_jX_i, \quad 1 \leqslant j < j+1 < i < r, \\ &X_i^2 - (q - q^{-1})X_i - 1, \quad i = 1, \ldots, r-1. \end{aligned} \tag{18}$$

Note the isomorphism between the Hecke algebra $\mathscr{H}_r(1)$ and the complex unital group algebra of the symmetric group S_r.

For instance, in the special case $r = 6$ the additional elements

$$\begin{aligned} &X_3X_5X_4X_3 - X_5X_4X_3X_4, \quad X_2X_4X_3X_2 - X_4X_3X_2X_3, \\ &X_1X_3X_2X_1 - X_3X_2X_1X_2, \quad X_2X_5X_4X_3X_2 - X_5X_4X_3X_2X_3, \\ &X_1X_4X_3X_2X_1 - X_4X_3X_2X_1X_2, \quad X_1X_5X_4X_3X_2X_1 - X_5X_4X_3X_2X_1X_2 \end{aligned}$$

have to be added to (18) in order to obtain a minimal $\mathfrak{A}$-Gröbner basis of K, where the order $\prec_A$ of the free word semigroup $\langle Y_1, Y_2, Y_3, Y_4, Y_5\rangle$ refines the total degree order extending $Y_5 \prec Y_4 \prec Y_3 \prec Y_2 \prec Y_1$ (cf. [12]). Note, any product $X_{i_1} \cdots X_{i_k}$ such that $k > 15$ is reducible with respect to the above Gröbner basis of K and the maximal irreducible product is $X_5X_4X_3X_2X_1X_5X_4X_3X_2X_5X_4X_3X_5X_4X_5$.

The Hecke algebra $\mathscr{H}_r(q)$ is a finite-dimensional $\mathbb{C}$-vector space for an arbitrary $r \geqslant 2$ whereby the monomials of degree at most $d := r(r-1)/2$ form a (non-minimal) generating set. A natural graded structure of $\mathscr{H}_r(q)$ with respect to a commutative valuation monoid does not satisfy condition (4). Using the free non-commutative valuation monoid $\langle Y_1, \ldots, Y_{r-1}\rangle$ the above theorem is not applicable since the monoid is not noetherian. A possible valuation monoid for building an effective left (right) Gröbner structure of the Hecke algebra $\mathscr{H}_r(q)$ is $\Gamma = \langle Y_1, \ldots, Y_{r-1}\rangle / E_d$, where E_d is the congruence relation defined by the equations $Y_{i_1} \cdots Y_{i_t} = Y_{i_{\pi(1)}} \cdots Y_{i_{\pi(t)}}$, for all $t > d$ and all

[11] To be precise, $\mathbb{C}$ has to be replaced by an arbitrary computable subfield in order to obtain an effective one-sided Gröbner structure.

permutations $\pi \in S_t$. The associated graded rings of the natural graded structures of $\mathscr{H}_r(q)$ with respect to $\langle Y_1, \ldots, Y_{r-1} \rangle$ and Γ, respectively, are graded isomorphic [12] and, hence, the Gröbner bases are the same with respect to both graded structures. But Γ is a noetherian (non-commutative) monoid satisfying the assumption of Theorem 6 (but not of Theorems 7 or 8) and provides algorithms for the computation of Gröbner bases of one-sided ideals of $\mathscr{H}_r(q)$.

A similar construction works for arbitrary finite-dimensional algebras R, in particular, for group algebras of finite groups.

Examples for Euclidean domains Q and coefficients not commutating with the generators X can be found in Section 14 (Examples 2 and 3).

12. Effective two-sided Gröbner structures

Under some additional assumptions the graded structures considered in Theorem 1 allow also the computation of Gröbner bases of two-sided ideals of R using a generalized Kandri-Rody/Weispfenning closure technique [17].

Theorem 7. *Let Q be a computable noetherian ring with decidable ideal membership and solvable syzygy problem for left, right, and two-sided ideals, and $\hat{Q}$ a subring of the center of Q such that Q is a computable $\hat{Q}$-module. Furthermore, let Γ be a computable well-ordered commutative monoid which is noetherian and allows algorithmic computation of minimal common multiples and factorial decompositions. In addition, let there exist computable functions $\kappa : Q \times Q \to Q$ and $\kappa_Y : Y \times Q \to Q$ satisfying $\alpha \cdot \beta = \kappa(\alpha, \beta) \cdot \alpha$ respectively $\alpha \cdot \mathfrak{g}_{Y_i} = \kappa_Y(Y_i, \alpha) \cdot \mathfrak{g}_{Y_i} \cdot \alpha$ for all $\alpha, \beta \in Q$ and $i = 1, \ldots, n$. Finally, let $R = \langle Q, X \rangle_{\hat{Q}}/K$ be given by a finite Γ-truncation H_{trunc} of a minimal $\mathfrak{A}$-Gröbner basis of K and the associated graded ring G of the natural graded structure $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in})$ satisfy conditions* (4) *and* (15).

Then $\mathfrak{R}$ is an effective two-sided Gröbner structure and each two-sided Gröbner basis F of an arbitrary two-sided ideal $I \subseteq R$ is also a left and a right Gröbner basis of I.

Proof. It remains to consider the solution of the syzygy problem. Note, $\hat{Q}$ is a subring of the center of R and the initial mapping acts identically on $\hat{Q}$. Therefore, according to the criterion presented behind Definition 3 it suffices to show that for an arbitrary finite set U of non-zero homogeneous elements of G there can be computed a finite homogeneous generating set of $\mathrm{Syz}_{\hat{Q}}(U)$ in an algorithmic way.

For arbitrary $\alpha \in Q$ and $u = \beta\mathfrak{g}_\gamma \in U$, where $\beta \in Q$ and $\gamma \in \Gamma$, there can be computed the syzygy $s_{\alpha,u} = e_u\alpha - \delta_{\alpha,u}e_u \in \mathrm{Syz}_{\hat{Q}}(U)$, where $\delta_{\alpha,u} = \kappa(\beta, \sigma_\gamma(\alpha))$. In a similar way there can be computed a syzygy $s_{Y_i,u} = e_u\mathfrak{g}_{Y_i} - \delta_{Y_i,u}\mathfrak{g}_{Y_i}e_u \in \mathrm{Syz}_{\hat{Q}}(U)$ for given $i = 1, \ldots, n$ and $u \in U$. $s_{Y_i,u}$ is uniquely determined up to a trivial summand $\beta\mathfrak{g}_{Y_i}e_u$,

[12] Both associated graded rings are direct sums of the same non-zero modules belonging to the same degrees.

where $\beta \in \mathrm{ann_L}\, G_{Y_i \circ \gamma}$. Since H_{trunc} is finite the set $Z = \{\zeta \in Q \,|\, X_i\zeta - \sigma_{Y_i}(\zeta)X_i + p_{i,\zeta} \in H_{\mathrm{trunc}}\}$ of all highest coefficients of the elements of type (7) contained in the Γ-truncated Gröbner basis H_{trunc} is finite, too. Moreover, Z generates Q as a ring over $\hat{Q}$. So, we can compute finite sets $B_Z = \{s_{\zeta,u} \,|\, (\zeta, u) \in Z \times U\}$ and $B_Y = \{s_{Y_i,u} \,|\, (Y_i, u) \in Y \times U\}$. Next we will show that $B_Z \cup B_Y \cup \mathrm{LSyz}(U) \otimes_{\hat{Q}} 1$ generates $\mathrm{Syz}_{\hat{Q}}(U)$.

We have $e_u\zeta_1 \cdots \zeta_k = (s_{\zeta_1,u} + \delta_{\zeta_1,u}e_u)\zeta_2 \cdots \zeta_k$ and by induction on k it follows $s_{\zeta_1 \cdots \zeta_k,u} \in GB_ZG$ for all $u \in U$ and all products $\zeta_1 \cdots \zeta_k$, where $\zeta_1, \ldots, \zeta_k \in Z$. Hence, $s_{\alpha,u} \in GB_ZG$ for all $\alpha \in Q$ and $u \in U$. Next, we will prove the existence of a syzygy $s_{\gamma,u} = e_u\mathfrak{g}_\gamma - \delta_{\gamma,u}\mathfrak{g}_\gamma e_u \in G(B_Z \cup B_Y)G$ for all $\gamma \in \Gamma$ and $u \in U$ by induction on the length k of an arbitrary representation $\gamma = Y_{i_1} \circ \cdots \circ Y_{i_k}$. The initial step $k = 1$ is obvious. Consider $k > 1$ and set $\gamma' = Y_{i_1} \circ \cdots \circ Y_{i_{k-1}}$. We have $e_u\mathfrak{g}_{\gamma' \circ Y_{i_k}} = e_u\mathfrak{g}_{Y_{i_k}}\mathfrak{g}_{\gamma'}\alpha = s_{Y_{i_k},u}\mathfrak{g}_{\gamma'}\alpha + \delta_{Y_{i_k},u}\mathfrak{g}_{Y_{i_k}}e_u\mathfrak{g}_{\gamma'}\alpha$ for some $\alpha \in Q$ and by induction hypothesis there exists $s_{\gamma',u} = e_u\mathfrak{g}_{\gamma'} - \delta_{\gamma',u}\mathfrak{g}_{\gamma'}e_u \in G(B_Z \cup B_Y)G$. Hence, $e_u\mathfrak{g}_{\gamma' \circ Y_{i_k}} = s_{Y_{i_k},u}\mathfrak{g}_{\gamma'}\alpha + \delta_{Y_{i_k},u}\mathfrak{g}_{Y_{i_k}}s_{\gamma',u}\alpha + \delta_{Y_{i_k},u}\mathfrak{g}_{Y_{i_k}}\delta_{\gamma',u}\mathfrak{g}_{\gamma'} e_u\alpha = s_{Y_{i_k},u}\mathfrak{g}_{\gamma'}\alpha + \delta_{Y_{i_k},u}\mathfrak{g}_{Y_{i_k}}s_{\gamma',u}\alpha + \delta_{Y_{i_k},u}\mathfrak{g}_{Y_{i_k}}\delta_{\gamma',u}\mathfrak{g}_{\gamma'}s_{a,u} + \delta_{Y_{i_k},u}\mathfrak{g}_{Y_{i_k}}\delta_{\gamma',u}\mathfrak{g}_{\gamma'}\delta_{\alpha,u}e_u$. This finishes the induction proof. As an immediate consequence we obtain that for any homogeneous syzygy $s \in \mathrm{Syz}_{\hat{Q}}(U)$ there exists a homogeneous left syzygy $s' \in \mathrm{LSyz}(U)$ such that $s - s' \otimes 1 \in G(B_Z \cup B_Y)G$. Therefore, $B_Z \cup B_Y \cup \mathrm{LSyz}(U) \otimes_{\hat{Q}} 1$ generates $\mathrm{Syz}_{\hat{Q}}(U)$. $\mathrm{LSyz}(U)$ is computable according to Theorem 6. In conclusion, $\mathfrak{R}$ is an effective two-sided Gröbner structure.

From the above investigations it follows that for arbitrary homogeneous elements $u, v \in G$ there exists a homogeneous element $w \in G$ of the same degree as v such that $uv = wu$. Hence, any homogeneous left ideal of G is even two-sided. Therefore, left and two-sided initial ideal coincide for any two-sided ideal $I \subseteq R$. Moreover, the left and the two-sided ideal generated by the initial parts of a subset of I are equal. Consequently, any Gröbner basis of the two-sided ideal I is also a Gröbner basis of I considered as left ideal according to Definition 1. Analogous arguments apply to I considered as a right ideal. □

The requirement of the existence of the functions κ and κ_Y might seem rather technical. It could be replaced by one of the stronger conditions that Q is a skew field or $Q = \hat{Q}$. In fact these both situations are the most interesting applications.

Roughly, the idea behind the Kandri-Rody/Weispfenning closure technique consists in computing left Gröbner bases and checking whether the generated left ideal is closed under multiplication with variables from the right. If this is not the case then the nonzero remainders are added to the basis and the cycle of left Gröbner basis computation and saturation with right multiples is repeated. In our situation the generating set $B_Z \cup B_Y \cup \mathrm{LSyz}(U) \otimes_{\hat{Q}} 1$ of the syzygy module allows a similar procedure. The syzygies contained in B_Z and B_Y represent the multiples considered in the saturation step of the left Gröbner basis.

In the previous section we remarked the existence of Gröbner structures which are effective only with respect to one side. An interesting open question is if we can relax the conditions on Q in order to obtain graded structures which are an effective Gröbner structure with respect to two-sided and left (or right) ideals but not with respect to right (or left) ideals. Outside the theory of graded structures such a behavior is known from the investigations of Madlener and Reinert in group rings (see [20]).

Some classical examples satisfying the assumptions of Theorem 7 were already discussed in Section 11. Here, we will add only one remark concerning Hecke algebras. In fact, Gröbner bases of two-sided ideals in Hecke algebras can be computed without any problem by adding elements (18) to the ideal basis and computing a Gröbner basis in the graded structure (III). Though, (III) is not an effective Gröbner structure the method will be successful for the above particular ideals since after completion of (18) to a Gröbner basis only finitely many words remain as possible highest words for further Gröbner basis elements. In fact, it is a (cumbersome and tedious but not very difficult) exercise to generalize Theorem 7 to non-commutative valuation monoids which are "commutative for sufficiently large elements".

Mora considered a class of non-commutative algebras which allow the computation of Gröbner bases for two-sided but not necessarily for one-sided ideals (see [24]). The reason is that the associated graded ring satisfies the ascending chain condition for two-sided but not for one-sided ideals. The following theorem based on condition (16) generalizes Mora's result.

Theorem 8. *Let Q be a computable noetherian commutative ring with decidable ideal membership and solvable syzygy problem. Furthermore, let Γ be a computable well-ordered commutative monoid which is noetherian and allows algorithmic computation of minimal common multiples and factorial decompositions. Finally, let $R=\langle Q,X\rangle_Q/K$ be given by a finite Γ-truncation H_{trunc} of a minimal $\mathfrak{A}$-Gröbner basis of the two-sided ideal K and let the associated graded ring G of the natural graded structure $\mathfrak{R}=(R,\Gamma,\varphi,G,\mathrm{in})$ satisfy conditions* (4) *and* (16).

Then $\mathfrak{R}$ is an effective two-sided Gröbner structure.

Proof. The verification of condition (iv) of Definition 3 remains. We will sketch only the main ideas of the rather technical and lengthy proof and refer to Apel [5, Theorem 5.23] for the complete proof. First, we generalize set (17). Let $\gamma'\circ\gamma\circ\gamma''=\omega$ and γ',γ'' satisfy the assumptions of condition (16). In particular, we have $G_{\gamma'}G_\gamma=G_{\gamma'\circ\gamma}$ and $G_{\gamma'\circ\gamma}G_{\gamma''}=G_\omega$. Applying similar arguments as in the previous section to arbitrary $\omega',\omega''\in\Gamma$ we obtain an epimorphism sequence

$$G_\gamma\simeq Q/\mathrm{ann_R}\,G_\gamma\to Q/\mathrm{ann_R}\,G_{\gamma'\circ\gamma}\simeq Q/\mathrm{ann_L}\,G_{\gamma'\circ\gamma}\to Q/\mathrm{ann_L}\,G_\omega\to G_{\omega'\circ\omega\circ\omega''}.$$

Hence, for all $\gamma\in\Gamma$ the set

$$\hat{\Gamma}_\gamma=\{\omega\in\Gamma:\ \gamma|\omega\wedge G_\gamma\not\simeq G_\omega\}\tag{19}$$

is either empty or a monoid ideal of Γ. A finite generating set Δ_γ of $\hat{\Gamma}_\gamma$ can be computed using a Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis of K.

Now, we sketch the computation of a homogeneous generating set of the syzygy module $\mathrm{Syz}_Q(U)$. For any $Y_i\in Y$ and $u\in U$ there exists a homogeneous syzygy $s_{Y_i,u}=\alpha_{Y_i,u}e_u\mathfrak{g}_{Y_i}-\beta_{Y_i,u}\mathfrak{g}_{Y_i}e_u\in\mathrm{Syz}_Q(U)$, where at least one of the elements $\alpha_{Y_i,u},\beta_{Y_i,u}\in Q$ is a unit. Let $B_Y = \{s_{Y_i,u} \mid (Y_i, u) \in Y \times U\}$. For any homogeneous syzygy $s = \sum_{i=1}^{k} v_i e_{u_i} w_i \in \mathrm{Syz}_{\hat{Q}}(H)$ whose degree is a multiple of the degrees of all $u \in U$ there exists a homogeneous syzygy $s' = \mathrm{g}_\delta(\sum_{i=1}^{k} v_i' e_{u_i} w_i')\mathrm{g}_{\delta'}$ such that $s - s' \in GB_YG$ and $\deg(v_i') \circ \deg(u_i) \circ \deg(w_i')$ is a minimal common multiple of the degrees of the elements of U. Let $\Omega(U)_0$ be the set of all minimal common multiples of the degrees of $u \in U$ and define recursively $\Omega(U)_{i+1} = \bigcup_{\gamma \in \Omega(U)_i} \Delta_\gamma$. Then the set $\Omega(U) = \bigcup_{i=0}^{\infty} \Omega(U)_i$ is finite and can be constructed algorithmically. Finally, the set $B_Y \cup \bigcup_{\gamma \in \Omega(U)} C_\gamma \cup \bigcup_{U' \subset U} \mathrm{Syz}_Q(U')$, where the C_γ are finite generating sets of the Q-modules of all homogeneous syzygies of U of degree γ, generates $\mathrm{Syz}_Q(U)$. $\square$

Consider a quotient ring $R = Q\langle X_1, \ldots, X_n\rangle / K$ defined by a $\mathfrak{A}$-Gröbner basis of K of the shape $\{\underline{X_i X_j} - c_{i,j} X_j X_i + p_{i,j} \mid 1 \leqslant j < i \leqslant n\}$, the underscore marks the highest monomials with respect to $\prec_A$, and let $\mathfrak{R}$ denote a natural graded structure of R and $\Gamma = \mathbb{N}^n$. In contrast to Theorem 7 the assumptions of Theorem 8 allow also non-units among the $c_{i,j}$.[13] For instance, let $Q = \mathfrak{K}$ be a computable field and R the $\mathfrak{K}$-algebra defined by the two-sided ideal $K \subset A = \mathfrak{K}\langle X_1, \ldots, X_n\rangle$ with $\mathfrak{A}$-Gröbner basis $\{X_2X_1 - X_1X_2 - X_1, X_3X_1 + 1, X_3X_2 - X_2X_3 - X_3\}$. Then R is an example satisfying the assumptions of Theorem 8 which belongs to the class considered by Mora. Examples 1 and 4 of Section 14 illustrate the more general situation, where Q is not a field.

13. Open problems

Before we could prove that a natural graded structure $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in})$ is an effective Gröbner structure we had to introduce a series of conditions on the objects Q, Γ, and K. In this section we deal with the question which conditions could be relaxed without loosing the effective Gröbner structure property. For natural graded structures $\mathfrak{R}$ which are left, right, and two-sided Gröbner structure our conditions on Q are necessary and cannot not be relaxed in any way. If $\mathfrak{R}$ is required to be an effective Gröbner structure with respect to only one side, left, right, or two-sided, then the necessity of the conditions follows only for ideals of Q belonging to the same side. Under the condition that the natural graded structure of the monoid ring $Q\langle\Gamma\rangle$ has to be an effective Gröbner structure similar statements apply to the assumptions on Γ. In marginal cases with many homogeneous summands of G being the zero module, e.g. if $G_\gamma = 0$ for all $\gamma \in \Gamma \setminus \{\varepsilon\}$, the conditions on Γ could be relaxed. But in such situations the linkage between the ring R and the monoid Γ is so weak that often a graded structure of R with respect to a suitable submonoid of Γ satisfying our assumptions can be used. Open questions are when such a submonoid exists and how it can be constructed. Moreover, special situations with ground rings Q and valuation monoids Γ satisfying only the conditions corresponding to ideals of a fixed side remain open for future investigations.

[13] A necessary and sufficient condition which $c_{i,j}$ need not to be invertible was given in Section 10.

In Section 7, we gave examples showing that the restriction to graded structures whose associated graded ring has cyclic homogeneous summands is serious. But, in spite the described examples, this condition is very typical for Gröbner basis investigations. Even Pesch makes use of it by mainly working with the left module structure. Nevertheless, there remains an open research direction.

The condition that R has to be given by a finite Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis of the kernel K of a homomorphism $\iota : \langle Q,X\rangle_{\hat{Q}} \to R$ and conditions (15) and (16) are the most interesting restrictions and will be discussed now.

Assume, there exists an infinite sequence $\gamma_1, \gamma_2, \ldots \in \Gamma$ of right multiples such that $G_{\omega_i} G_{\gamma_i} \subsetneq G_{\gamma_{i+1}}$, where $\gamma_{i+1} = \omega_i \circ \gamma_i$, for all $i = 1, 2, \ldots$. Then the left ideal $G \cdot (\mathfrak{g}_{\gamma_1}, \mathfrak{g}_{\gamma_2}, \ldots)$ is not finitely generated. Hence, such a sequence cannot exist in the associated graded ring of an effective left Gröbner structure. Though, an effective left Gröbner structure need not necessarily satisfy condition (15) the above observation shows that the cases lying outside are rather marginal.

In the following, we will consider the condition that K can be presented by a finite Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis. If the ring Q is finitely generated over $\hat{Q}$ and there exists a finite confluent system of rewriting rules for Γ then there are $\mathfrak{A}$-Gröbner bases of K which contain only finitely many elements of types (7) and (8) and it remains to consider the number of elements of type (9). For effective left Gröbner structures there can be computed a finite homogeneous generating set of the left syzygy module of the principal left ideal generated by $\mathfrak{g}_\gamma \in G$ for any given $\gamma \in \Gamma$. The coefficients of the left syzygies of degree γ generate the annihilating left ideal of the homogeneous summand G_γ of the associated graded ring and, hence, the annihilating left ideals $\mathrm{ann}_{\mathrm{L}}\, G_\gamma$ are computable for any effective left Gröbner structure $\mathfrak{R}$ satisfying the above assumptions. Moreover, all $\omega \in \Gamma$ which are minimal right multiples of γ with the property that there exists a non-injective epimorphism from G_γ onto G_ω appear among the degrees of the left syzygies in an arbitrary homogeneous generating set of $\mathrm{LSyz}(G \cdot \mathfrak{g}_\gamma)$. Hence, if (15) holds then a finite generating set Δ_γ of the left monoid ideal (or empty set) Γ_γ defined in (17) can be computed in an algorithmic way for any given $\gamma \in \Gamma$. If $G_\gamma \simeq G_\omega$ for some proper divisor ω of $\gamma \in \Gamma$ then no elements of type (9) with highest degree γ need to be contained in a Γ-truncation H_{trunc}. Hence, we have to compute the set of all $\gamma \in \Gamma$ such that $G_\gamma \not\simeq G_\omega$ for all proper divisors ω. Let $\Omega(\{1\})$ be defined as in Section 11 before Theorem 6. $\Omega(\{1\})$ can be computed in an algorithmic way since it requires only computations of generating sets Δ_γ. Moreover, $\Omega(\{1\})$ is just the set of degrees where elements of type (9) can appear in a $\mathfrak{A}_\Gamma$-Gröbner basis of K. For each of the finitely many elements $\gamma \in \Omega(\{1\})$ there can be computed a finite generating set of $\mathrm{ann}_{\mathrm{L}}\, G_\gamma$. A possible set of highest coefficients of Gröbner basis elements of type (9) with highest term $X_{i_1} \cdots X_{i_k}$, where $Y_{i_1} \cdots Y_{i_k} \in \langle Y\rangle$ is the minimal representant of γ, can be found among the generators of $\mathrm{ann}_{\mathrm{L}}\, G_\gamma$. Note, we proved not only the existence of a finite Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis of K but also showed how its initial forms can be constructed whenever $\mathfrak{R}$ is an effective left Gröbner structure.

Similar considerations can be done in the two-sided case. In fact, the remaining gaps are larger than here, but, the most interesting cases are again covered by our theorems.

14. Examples

We already mentioned the classical applications of our theorems, e.g. polynomial rings over fields, enveloping algebras of Lie algebras, Weyl algebras, Hecke algebras, Clifford algebras, exterior algebras, etc., which have in common that the coefficient domains are fields. Moreover, our theorems apply also to the examples of polynomial rings over more general coefficient rings, e.g. Euclidean domains, which have been considered in the literature in the past.

The following examples will illustrate some typical new situations where our results are applicable, too. By considering rings R with more general coefficient rings Q and more general multiplicative structure than polynomial rings we show how our framework covers and unifies both classical research directions. Theorems 6–8 assumed that a finite Γ-truncation of a minimal $\mathfrak{A}$-Gröbner basis of K is given a priori. However, also if $R = A/K$ is given by an arbitrary finite generating set of K there is a good chance to compute a Γ-truncation of a Gröbner basis of K. There has to be calculated a (truncated) Gröbner basis in a free extension ring $A = \langle Q, X \rangle_{\hat{Q}}$ with the free word semigroup $\langle Y \rangle$ as valuation monoid. The decision of ideal membership and the computation of syzygy modules of finitely generated $\langle Y \rangle$-homogeneous ideals requires only the application of simple well-known algorithms for $\langle Y \rangle$-graded rings. Hence, the general method for computing Gröbner bases in graded structures becomes semi-algorithmic for free extension rings A, i.e. if there exists a finite $\mathfrak{A}$-Gröbner basis of K then it will be computed in finite time. If K has no finite $\mathfrak{A}$-Gröbner basis but a finite $\mathfrak{A}_\Gamma$-Gröbner basis then eventually the Gröbner method will have computed one. However, it is a (probably undecidable) problem to realize that the algorithm can be stopped. The examples were calculated using the special computer algebra system FELIX (see [7]).

Example 1. Consider the ring $A = \mathbb{Z}\langle x, y, z \rangle = \langle \mathbb{Z}, \{x, y, z\} \rangle_{\mathbb{Z}}$ which is freely generated by $\{x, y, z\}$ in the class of all extension rings of the integers $\mathbb{Z}$.[14] Let $\langle x, y, z \rangle$ denote the word monoid and Γ the monoid of commutative terms in the variables $\{x, y, z\}$. We order Γ by the total degree order $\prec$ extending $z \prec y \prec x$ and $\langle x, y, z \rangle$ by the well-founded order $\prec_A$ which compares the words first (forgetting non-commutativity) according to $\prec$ and second applies the lexicographical order $<_1$ extending $x <_1 y <_1 z$ for breaking ties. Let $\mathfrak{A}$ denote the natural $\langle x, y, z \rangle$-graded structure of A and consider the two-sided ideal $K \subseteq A$ generated by $\{yx - 3xy - 3z, zx - 2xz + y, zy - yz - x\}$. During the computation of a $\mathfrak{A}$-Gröbner basis of K the following elements are constructed:

$$yx - 3xy - 3z, zx - 2xz + y, zy - yz - x,$$

$$6yz + 3x, 9xz - 3y, 12xy + 9z, 12y^2 - 27z^2, x^2 + 2y^2 - 6z^2,$$

$$9z^3 - 30xy - 21z, 4y^3 + 9yz^2 + 3y, 4xy^2 + 3yz + 3x, 3xyz - 3y^2 + 9z^2,$$

[14] Note, the condition that $\mathbb{Z}$ is contained in the center of A is trivially satisfied since only rings with unit element are considered.

$$3yz^3 - 90xy^2 - 3xz^2 - 3yz - 36x, 2y^3z - 3xy^2 + 3yz, xy^2z - 3y^3 - 3xz,$$

$$y^3z^3 - 2xy^4 - 3y^3z - 3yz^3 + xy^2 - 3yz,$$

$$xy^3z + 3y^4 - 6y^2z^2, xy^4z + y^5 + y^3z^2 + 2y^3 - 3yz^2, xy^5z - y^6 + 3y^4z^2, \ldots$$

Reducing $(xy^{j-1}z + p_{j-1})y$ modulo this intermediate basis we observe by induction that K contains an element of the form $xy^jz + p_j$, where $\varphi_A(p_j) \prec_A xy^jz$, for any positive integer $j > 1$. In fact, only such elements are necessary in order to complete the above intermediate basis to an infinite $\mathfrak{A}$-Gröbner basis of K but a finite $\mathfrak{A}$-Gröbner basis does not exist. However, the above set is already a $\mathfrak{A}_\Gamma$-Gröbner basis of K, i.e. it is a Γ-truncation of a $\mathfrak{A}$-Gröbner basis of K. Even the elements of the last row can be dropped. The ring $R = A/K$ satisfies the assumptions of Theorem 8 and therefore, the natural Γ-graded structure of R is an effective two-sided Gröbner structure. The assumptions of Theorems 5 and 7 are violated since the coefficient of xy in $yx - 3xy - 3z$ is not invertible modulo the annihilating ideal $\mathrm{ann}_{\mathrm{L}}\, G_{xy} = 12\mathbb{Z}$.

Example 2. Consider the graded structure $\mathfrak{A}$ from the previous example and let K be the two-sided ideal generated by the elements $yx - 3xy - z, zx - xz + y$, and $zy - yz - x$. We are interested in the natural Γ-graded structure of $R = A/K$. The generators look similar to the defining relations of an algebra of solvable type. But even if we allow rational coefficients the behavior of our ring is much different since the terms $x^iy^jz^k$ $(i, j, k = 0, 1, 2, \ldots)$ are linearly dependent. The elements

$$yx - 3xy - z, zx - xz + y, zy - yz - x,$$

$$8xy + 2z, 4xz - 2y, 4yz + 2x,$$

$$2x^2 - 2y^2, 4y^2 - 2z^2, 2z^3 - 2xy$$

form a finite $\mathfrak{A}$-Gröbner basis of the two-sided ideal $K \subset \mathbb{Z}\langle x, y, z\rangle$, where $\mathfrak{A}$ denotes the graded structure introduced in Example 1. Since $\mathrm{ann}_{\mathrm{L}}\, G_{xy} = 8\mathbb{Z}$, we have $\mathfrak{g}_{xy} = \mathfrak{g}_x\mathfrak{g}_y = 3\mathfrak{g}_y\mathfrak{g}_x$ in the associated graded ring of the natural Γ-graded structure $\mathfrak{R}$ of R. Hence, condition (15) holds. The other assumptions of Theorem 7 are obvious. Consequently, finite Gröbner bases with respect to $\mathfrak{R}$ can be computed for arbitrary ideals of R using the algorithms sketched in this paper.

Example 3. Let the coefficient ring $\mathscr{W} = \mathbb{Q}\langle p, q\rangle/(qp - pq - 1)$ be a non-commutative ring similar to a Weyl algebra but with coefficients restricted to rational numbers. Consider the ring $R = \langle \mathscr{W}, \{x, y\}\rangle_{\mathbb{Q}}/K$, where K is the two-sided ideal of $\langle \mathscr{W}, \{x, y\}\rangle_{\mathbb{Q}}$ given by the Gröbner basis

$$xp - qx, xq + px, yp - qy, yq + py, yx - xy + y^2$$

with respect to the natural graded structure induced by the well-ordered word monoid $(\langle x, y\rangle, \prec_A)$, where $\prec_A$ compares words by first forgetting non-commutativity and applying the lexicographical order $\prec$ of the free commutative monoid which extends $y \prec x$

and second breaking ties by comparing the non-commutative words with respect to the lexicographical order extending $x <_1 y$. Note, not all coefficients but only the rational numbers commute with the variables of the ring R. Functions κ and κ_Y as required in Theorem 7 do not exist but at least the assumptions of Theorem 6 are fulfilled in this situation. For this reason finite Gröbner bases of left ideals $I \subseteq R$ can be computed using the algorithms presented in this paper. Consider the homogeneous element $u = p\mathfrak{g}_{x^2y}$ of the associated graded ring G of R. Since $up - au = (-pq - ap)\mathfrak{g}_{x^2y} \neq 0$ for all $a \in \mathscr{W}$ the two-sided ideal generated by u is strictly larger than the left ideal generated by u. Hence, homogeneous left ideals of G need not to be two-sided and, therefore, two-sided Gröbner bases need not to be left Gröbner bases. However, though neither Theorem 7 nor Theorem 8 are applicable it remains an open question if the natural graded structure of R is an effective two-sided Gröbner structure.

Example 4. Once again, let us consider the graded structure $\mathfrak{A}$ from Example 1 and let K be generated by $yx - 3xy, zx + y^2, zy - yz + z^2$. Since $R = A/K$ is a $\mathbb{N}$-graded ring it is easy to observe that $\operatorname{ann}_{\mathrm{L}} G_{xz}$ and $\operatorname{ann}_{\mathrm{L}} G_{xy}$ are zero ideals. Therefore, the coefficient 3 of xy in the first generator and the coefficient 0 of xz in the second generator are both not invertible modulo the corresponding annihilating left ideal and, hence, neither Theorem 6 nor Theorem 7 can be applied to R. The elements

$$yx - 3xy, zx + y^2, zy - yz + z^2,$$

$$2y^3 + y^2z - 2yz^2 + 2z^3,$$

$$14yz^3 - 28z^4, y^2z^2 - 4yz^3 + 6z^4, 27xy^2z - 54xyz^2 + 54xz^3 + y^4,$$

$$14z^5, 2yz^4 - 6z^5, y^4z, y^5, 2xyz^3 - 4xz^4, 27xy^3z,$$

$$2z^6, 2xz^5$$

form a $\mathfrak{A}$-Gröbner basis of K. Consider arbitrary monoid elements $\omega = x^i y^j z^k$ and $\gamma = x^{i'} y^{j'} z^{k'}$ such that $\gamma \mid \omega$. Then condition (16) holds for the decomposition $\gamma' \circ \gamma \circ \gamma''$, where $\gamma' = x^{i-i'}$ and $\gamma'' = y^{j-j'} z^{k-k'}$. Hence, the assumptions of Theorem 8 are satisfied and the natural Γ-graded structure $\mathfrak{R}$ of R is an effective two-sided Gröbner structure. A finite Gröbner basis can be computed for any two-sided ideal of R using the algorithms sketched in this paper.

Note, R does not satisfy the ascending chain condition for left ideals, e.g. the left ideal $R(xz, xz^2, xz^3, \ldots)$ has no finite generating set. Hence, it is proved that $\mathfrak{R}$ is not an effective left Gröbner structure.

Acknowledgements

The author is grateful to Teo Mora and the two anonymous referees for valuable remarks and hints on a previous version of this paper.

References

[1] W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Mathematics, vol. 3, AMS Press, Providence, 1994.
[2] J. Apel, Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung, Ph.D. Thesis, University of Leipzig, 1988.
[3] J. Apel, A relationship between Gröbner bases of ideals and vector modules of G-algebras, Contemp. Math. 131/2 (1992) 195–204.
[4] J. Apel, Effective Gröbner structures, Report No. 12, Institute of Computer Science, University of Leipzig, 1997.
[5] J. Apel, Zu Berechenbarkeitsfragen der Idealtheorie, Habilitationsschrift, University of Leipzig, 1998.
[6] J. Apel, Computational ideal theory in finitely generated extension rings, Report No. 12, Institute of Computer Science, University of Leipzig, 1998.
[7] J. Apel, U. Klaus, FELIX – an assistant for algebraists, Proc. ISSAC'91, ACM Press, New York, 1991, pp. 382–389.
[8] J. Apel, W. Laßner, An extension of Buchberger's algorithm and calculations in enveloping fields of lie algebras, J. Symbolic. Comput. 6 (1988) 361–370.
[9] T. Becker, V. Weispfenning, (in cooperation with H. Kredel), Gröbner Bases, A Computational Approach to Commutative Algebra, Springer, New York, 1993.
[10] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. Thesis, University of Innsbruck, 1965.
[11] B. Buchberger, A Critical Pair/Completion Algorithm in Reduction Rings, Lecture Notes in Computer Science, vol. 171, Springer, Berlin, 1983, pp. 137–161.
[12] B. Buchberger, An algorithmic method in polynomial ideal theory, in: N.K. Bose (Ed.), Recent Trends in Multidimensional System Theory, D. Reidel, Dordrecht, 1985 (Chapter 6).
[13] L.E. Dickson, Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors, Amer. J. Math. 35 (1913) 413–426.
[15] H. Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero, Ann. Math. 79 (1964) 109–326.
[16] A. Kandri-Rody, D. Kapur, Algorithms for Computing Gröbner Bases of Polynomial Ideals over Various Euclidean Rings, Lecture Notes in Computer Science, vol. 174, Springer, Berlin, 1984, pp. 193–206.
[17] A. Kandri-Rody, V. Weispfenning, Non-commutative Gröbner bases in algebras of solvable type, J. Symbolic. Comput. 9/1 (1990) 1–26.
[18] H. Kredel, Solvable polynomial rings, Ph.D. Thesis, University of Passau, Shaker, 1992.
[19] K. Madlener, B. Reinert, Computing Gröbner bases in monoid and group rings, Proc. ISSAC'93, ACM Press, New York, 1993, pp. 254–263.
[20] K. Madlener, B. Reinert, A generalization of Gröbner basis algorithms to polycyclic group rings, J. Symbolic. Comput. 25 (1998) 23–44.
[21] H.M. Möller, On the construction of Gröbner bases using syzygies, J. Symbolic. Comput. 6 (1988) 345–359.
[22] H.M. Möller, T. Mora, New constructive methods in classical ideal theory, J. Algebra 100 (1986) 138–178.
[23] T. Mora, Seven Variations on Standard Bases, Preprint, Univ. di Genova, Dip. di Mathematica, No. 45, 1988.
[24] T. Mora, Gröbner Bases in Non-Commutative Algebras, Lecture Notes in Computer Science, vol. 358, Springer, Berlin, 1989, pp. 150–161.
[25] L. Pan, Application of rewriting techniques, Ph.D. Thesis, University of Santa Barbara, 1985.
[26] M. Pesch, Gröbner bases in skew polynomial rings, Ph.D. Thesis, University of Passau, Shaker, 1998.
[27] L. Robbiano, On the theory of graded structures, J. Symbolic. Comput. 2 (1986) 139–170.
[28] A. Rosenman, An algorithm for constructing Gröbner and free schreier bases in free group algebras, J. Symbolic. Comput. 16 (1993) 523–549.
[29] S.C. Schaller, Algorithmic aspects of polynomial residue class rings, Ph.D. Thesis, University Wisconsin at Madison, 1979.

[30] S. Stifter, A generalization of reduction rings, J. Symbolic Comput. 4/3 (1987) 351–364.
[31] W. Trinks, Über Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen, J. Number Theory 10 (1978) 475–488.
[32] G. Zacharias, Generalized Gröbner bases in commutative polynomial rings, Bachelor Thesis, MIT, Boston, 1978.