Bachelor of Science Thesis

Letterplace Gröbner Bases, their Implementation and Applications

Karim Josef Abou Zeid

The present work was submitted to the LuFG Theory of Hybrid Systems

March 25, 2019

Examiners:
Prof. Dr. Erika Ábrahám
Priv.-Doz. Dr. Viktor Levandovskyy

Abstract

We give a complete introduction to Gröbner basis theory in the free associative algebra $K\langle X\rangle$. Moreover, we introduce the Letterplace ring, a tool which allows us to perform computations from $K\langle X\rangle$ in the commutative polynomial ring instead. The algorithm in the computer algebra system SINGULAR that computes Gröbner bases in $K\langle X\rangle$ is built on top of Letterplace. Let I be an ideal of $K\langle X\rangle$. We have extended the algorithm in SINGULAR to also compute right Gröbner bases in $K\langle X\rangle/I$.

Further on, we have discovered that depending on the monomial ordering, the Gelfand-Kirillov dimension of $K\langle X\rangle/I$ is not necessarily the same as the Gelfand-Kirillov dimension of $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$. Finally, we propose a new algorithm to compute the Gelfand-Kirillov dimension of $K\langle X\rangle/I$.

Zusammenfassung

Wir geben eine vollständige Einführung zur Gröbnerbasis Theorie in der freien assoziativen Algebra $K\langle X\rangle$. Außerdem stellen wir den Letterplace Ring vor, ein Werkzeug, mit dem wir Berechnungen in $K\langle X\rangle$ stattdessen im kommutativen Polynomring tätigen können. Der Algorithmus im Computeralgebrasystem SINGULAR, der die Gröbnerbasen in $K\langle X\rangle$ berechnet, basiert auf Letterplace. Sei I ein Ideal von $K\langle X\rangle$. Wir haben den Algorithmus in SINGULAR erweitert, um auch rechts Gröbnerbasen in $K\langle X\rangle/I$ zu berechnen.

Desweiteren haben wir entdeckt, dass abhängig von der Monomordnung, die Gelfand-Kirillov-Dimension von $K\langle X\rangle/I$ nicht unbedingt mit der Gelfand-Kirillov-Dimension von $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ übereinstimmt. Schließlich schlagen wir einen neuen Algorithmus vor, um die Gelfand-Kirillov-Dimension von $K\langle X\rangle/I$ zu berechnen.

Acknowledgments

First of all, I would like to thank Priv.-Doz. Dr. Viktor Levandovskyy who proposed the topic to me, was always there to answer my questions during this thesis and took his time to be my second examiner. Many thanks to Prof. Dr. Erika Ábrahám for giving me the opportunity to write this thesis.

I also have to thank Leonard Schmitz for his constructive feedback. Special thanks to Anna for providing me with emotional support. Last but definitely not least, I am grateful to my family for always supporting me.

Contents

Chapter 1

Introduction

In this thesis we study noncommutative Gröbner bases in the free associative algebra $K\langle X\rangle$ and the implementation of the algorithm to compute them in the computer algebra system SINGULAR. Moreover, we use Gröbner bases and the Ufnarovski graph to compute the Gelfand-Kirillov dimension and the K-dimension of the factor algebra $K\langle X\rangle/I$.

In Chapter 2 we introduce the free associative algebra $K\langle X\rangle$, which is the main algebraic object we will be working with. Furthermore, we introduce the two most important ingredients for Gröbner basis theory, these are monomial orderings and a reduction procedure.

In Chapter 3 we give a detailed introduction to Gröbner bases in $K\langle X\rangle$. Our main reference for this chapter is [Nor01a]. We investigate when a set of polynomials is a Gröbner basis and construct an algorithm to compute Gröbner bases in $K\langle X\rangle$ as in [Nor01a]. Moreover, we discuss several properties of Gröbner bases and see some basic applications. In Section 3.6 we turn to a more special case: right Gröbner bases in $K\langle X\rangle/I$. Our reference for this section is [Nor01b], where the completely symmetrical case of left Gröbner bases in $K\langle X\rangle/I$ is discussed.

Most of the previous are well know facts in this field. Our own contribution to this topic is in the following chapters.

In Chapter 4 we focus on the implementation of the Gröbner basis algorithms. First we introduce the Letterplace ring [LSL09], a tool which allows us to perform computations from $K\langle X\rangle$ in the commutative polynomial ring instead. Then we provide a rather detailed overview of the implementation of the Gröbner basis algorithm in SINGULAR via Letterplace which was not documented before in its current state. As a part of this thesis, we have extended the existing Gröbner basis algorithm in SINGULAR to compute right Gröbner bases in $K\langle X\rangle/I$ and give an overview on its implementation (Algorithm 6).

In Chapter 5 we use Gröbner bases and the Ufnarovski graph to compute the Gelfand-Kirillov dimension and the K-dimension of $K\langle X\rangle/I$. First we define the growth and the Gelfand-Kirillov dimension of algebras as in [KL99]. We discovered that depending on the monomial ordering, the Gelfand-Kirillov dimension of $K\langle X\rangle/I$ is not necessarily the same as the Gelfand-Kirillov dimension of $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ (Proposition 5.10, Lemma 5.12, Example 5.23). We give a sufficient condition for when they are equal, that is for example the case if the monomial ordering is length-compatible. Furthermore, we propose a new algo-

rithm that can be used to compute the Gelfand-Kirillov dimension of $K\langle X\rangle/I$ using the Ufnarovski graph (Algorithm 7). We have slightly improved the algorithm to compute the K-dimension of $K\langle X\rangle/I$ in [Xiu12] as well (Algorithm 9).

Chapter 2

Preliminaries

2.1 The Free Associative Algebra

The free associative algebra is the main structure that we will be working with. It is also sometimes called the "noncommutative polynomial ring". This is because the elements in the free associative algebra can be viewed as polynomials in noncommuting variables.

Given an alphabet X and using the Kleene star notation, the set X^* denotes the set of all words over X, including the empty word ε. By equipping X^* with the concatenation operation $\cdot$, that is $m_1 \cdot m_2 \coloneqq m_1 m_2$ for $m_1, m_2 \in X^*$, we get the free monoid $\langle X \rangle$. By $|w|$ we denote the length of a word w. We write $u \mid v$ if u is a subword of v. Respectively, we write $u \nmid v$ if u is not a subword of v. If $u \mid v$ we also say u *divides* v.

From now on, unless otherwise stated, let K be an arbitrary but fixed field and let X be an arbitrary but fixed (finite) alphabet. Recall that an algebra over K is a vector space over K equipped with a bilinear multiplication.

Definition 2.1. The *free associative algebra* $K\langle X \rangle$ is the vector space over K with the infinite basis $\langle X \rangle$. It becomes an algebra over K by defining a multiplication on the vectors as

$$\underbrace{\Big(\sum_{u \in \langle X \rangle} a_u u\Big)}_{\in K\langle X \rangle} \cdot \underbrace{\Big(\sum_{v \in \langle X \rangle} b_v v\Big)}_{\in K\langle X \rangle} \coloneqq \underbrace{\sum_{u,v \in \langle X \rangle} a_u b_v uv}_{\in K\langle X \rangle} = \sum_{w \in \langle X \rangle} \Big(\sum_{\substack{u,v \in \langle X \rangle \\ uv = w}} a_u b_v\Big) w,$$

and $a_u, b_v \in K$. As a convention, we write $K\langle x_1, \ldots, x_n \rangle$ instead of $K\langle \{x_1, \ldots, x_n\} \rangle$.

Remark. Because $K\langle X \rangle$ is a vector space, only finitely many $a_u, b_v \neq 0$.

Remark. The free associative algebra can also be defined over a ring instead of a field. The vector space is then replaced by a free module. This case, however, is not a part of this thesis.

Observation 2.2. The elements in $K\langle X \rangle$ are precisely the elements

$$\sum_{w \in \langle X \rangle} c_w w \quad \text{with } c_w \in K \text{ and only finitely many } c_w \neq 0.$$

Example 2.3. Suppose $K = \mathbb{Q}$ and $X = \{x, y\}$. Then

$$xyx + 3xxy = 3xxy + xyx \in \mathbb{Q}\langle x, y\rangle \quad \text{and} \quad xyx \neq xxy \in \mathbb{Q}\langle x, y\rangle.$$

We call the elements of X *variables* and the elements of $K\langle X\rangle$ *polynomials*. The elements of $\langle X\rangle$ are sometimes also referred to as *monomials* instead of words.

For convenience, we identify $1 \in K$ with the empty word $\varepsilon \in \langle X\rangle$. Then we have $c \cdot \varepsilon = c \in K\langle X\rangle$ for $c \in K$.

Definition 2.4. Let $f = \sum_{w\in\langle X\rangle} c_w w$ with $c_w \in K$ be a polynomial in $K\langle X\rangle$. We call c_w the *coefficient* of w in f. The *support* of f, denoted by $\operatorname{supp}(f)$, is the finite set $\{w \in \langle X\rangle \mid c_w \neq 0\}$.

Definition 2.5. The degree of a polynomial $f \in K\langle X\rangle$, denoted by $\deg(f)$, is the length of the longest word in $\operatorname{supp}(f)$. For convenience, we also define $\deg(c) \coloneqq 0$ for $c \in K \setminus \{0\}$ and $\deg(0) \coloneqq -\infty$.

Definition 2.6. Let A be an algebra. A vector subspace I of A is called

1. a *left ideal* of A if $f \cdot g \in A$ for all $f \in A$, $g \in I$,
2. a *right ideal* of A if $g \cdot f \in A$ for all $f \in A$, $g \in I$,
3. a *(two-sided) ideal*, or simply an *ideal*, of A if it is both a left and a right ideal of A.

Because an ideal of an algebra is a vector subspace, it cannot be empty. Every algebra hast at least two ideals, that is the zero ideal $\{0\}$ and the algebra itself.

Definition 2.7. Let A be an algebra. A subset $F \subset A$ is a *system of generators* of an ideal I of A if I is the smallest ideal of A containing F. In this case we have

$$I = \left\{ \sum_{i=1}^{k} l_i f_i r_i \mid f_i \in F,\ l_i, r_i \in A,\ k \in \mathbb{N} \right\}, \tag{2.1}$$

and we say F generates I, denoted by $\langle F\rangle = I$. If I can be generated by a finite system of generators, then we say I is *finitely generated*. As a convention, we write $\langle p_1, \ldots, p_n\rangle$ instead of $\langle\{p_1, \ldots, p_n\}\rangle$ for $p_1, \ldots, p_n \in A$.

Remark. Note that since A is not necessarily commutative, we cannot assume $f_i \neq f_j$ for $i \neq j$.

Remark. Definition 2.7 also applies to left ideals and right ideals but then we have $I = \{\sum_{i=1}^{k} l_i f_i \mid f_i \in F,\ l_i \in A,\ k \in \mathbb{N}\}$ and $I = \{\sum_{i=1}^{k} f_i r_i \mid f_i \in F,\ r_i \in A,\ k \in \mathbb{N}\}$ respectively.

Since we can expand l_i and r_i from (2.1) into words in $K\langle X\rangle$, we can write every polynomial in the ideal generated by $F \subset K\langle X\rangle$ as

$$\sum_{i=1}^{k} c_i u_i f_i v_i, \quad c_i \in K,\ u_i, v_i \in \langle X\rangle,\ f_i \in F.$$

Again, we cannot assume $f_i \neq f_j$ for $i \neq j$.

Let I be an ideal of $K\langle X\rangle$. Since I is a vector subspace of $K\langle X\rangle$, the quotient space $K\langle X\rangle/I \coloneqq \{f + I \mid f \in K\langle X\rangle\}$, where the addition is given by

$$(f + I) + (f' + I) = (f + f') + I,$$

for $f, f' \in K\langle X\rangle$, is well-defined. Moreover, we define the multiplication as

$$(f + I)(f' + I) = ff' + I,$$

for $f, f' \in K\langle X\rangle$. Then the quotient space $K\langle X\rangle/I$ becomes an algebra over K and is called the *factor algebra* (or *quotient algebra*) *of* $K\langle X\rangle$ *modulo* I. By the definition of the operations, the map $\nu\colon K\langle X\rangle \to K\langle X\rangle/I$ given by $f \mapsto f + I$ is a ring epimorphism with kernel I and we call $\nu(f)$ the image of f in $K\langle X\rangle/I$. If I is finitely generated, we say $K\langle X\rangle/I$ is *finitely presented*. This is a classical construction in algebra and a detailed explanation of factor rings can be found, for example, in [Xiu12] (Section 2.2).

2.2 Monomial Orderings

Monomial orderings are one of the cornerstones of Gröbner basis theory. They are essential for defining Gröbner bases as well as for the algorithms to compute them.

Definition 2.8. A *strict total ordering* $\prec$ on $\langle X\rangle$ is a relation such that

1. $w \prec w'$ and $w' \prec w''$ implies $w \prec w''$ for all $w, w', w'' \in \langle X\rangle$,
2. and either $w \prec w'$ or $w' \prec w$ for all $w, w' \in \langle X\rangle$ with $w \neq w'$.

Definition 2.9. A strict total ordering $\prec$ on $\langle X\rangle$ is a *well-ordering* if every non-empty subset of $\langle X\rangle$ has a least element.

Remark. Note that with a well-ordering on $\langle X\rangle$ there can be no infinite descending chain $w_1 \succ w_2 \succ \dots$ of words in $\langle X\rangle$.

Definition 2.10. A strict total well-ordering $\prec$ on $\langle X\rangle$ is a *monomial ordering* if it is compatible with the multiplication, that is, for all $w, w', u, v \in \langle X\rangle$ with $w \prec w'$ we have $uwv \prec uw'v$.

Remark. Monomial orderings are also often called *term orderings* or *admissible orderings*.

Note that with a monomial ordering, ε is always the smallest word in $\langle X\rangle$. Otherwise there would exists $w \in \langle X\rangle$ with $w \succ \varepsilon$ and $\varepsilon \succ w \succ w^2 \succ \dots$ would be an infinite descending chain of words.

Example 2.11 (degree left lexicographic ordering)**.** First, consider the *left lexicographic ordering*. The entries in a dictionary are left lexicographically ordered with respect to the alphabetical ordering of the letters. Let us assume that the letters in X are also ordered in some way. Then we say the word $w = x_{i_1} \cdots x_{i_k} \in \langle X\rangle$ is left lexicographically greater than the word $w' = x_{j_1} \cdots x_{j_t}$ if

1. there exists $u \in \langle X\rangle \setminus \{\varepsilon\}$ such that $w = w'u$, or

2. there exists $m < \min(|w|, |w'|)$ such that $x_{i_n} = x_{j_n}$ for all $n \leq m$ but x_{i_m} is greater than x_{j_m}.

However, the left lexicographic ordering is not a monomial ordering. Suppose $X = \{x, y\}$ and $x \succ y$, then $x \succ yx \succ y^2x \succ \ldots$ is an infinite descending chain of words. In order to resolve this problem, we first order the words ascending by their length and then left lexicographically to break ties. We call this ordering the *degree left lexicographic ordering* and it is indeed a monomial ordering.

Remark. Analogously one can define the *degree right lexicographic ordering*.

Remark. In the commutative case, the left (or right) lexicographic ordering is already a monomial ordering.

Example 2.12. Consider $K\langle X\rangle$ with $X = \{x, y\}$, $x \succ y$ and the degree left lexicographic ordering. Then $x^2y \succ xy^2 \succ xy \succ yx \succ y^2 \succ x$.

Definition 2.13. We say a monomial ordering $\prec$ is *length-compatible* if $|w| < |w'|$ implies $w \prec w'$ for all $w, w' \in \langle X\rangle$.

Note that the degree left lexicographic ordering is length-compatible.

Most properties defined in the following sections heavily depend on the monomial ordering that is used. Therefore, from now on we assume that an arbitrary but fixed monomial ordering $\prec$ on $\langle X\rangle$ is given.

Definition 2.14. Let f be a polynomial in $K\langle X\rangle \setminus \{0\}$. We can write f uniquely as

$$f = \sum_{i=1}^{k} c_i w_i, \quad c_i \in K \setminus \{0\},\ w_i \in \langle X\rangle, \quad w_i \succ w_{i+1} \text{ for all } i < k.$$

We define the *leading monomial* of f, denoted by $\mathrm{lm}(f)$, as w_1, the *leading coefficient* of f, denoted by $\mathrm{lc}(f)$, as c_1 and the *leading term* of f, denoted by $\mathrm{lt}(f)$, as c_1w_1.

Note that $\mathrm{lm}(0)$ and $\mathrm{lc}(0)$ are undefined. For a set of polynomials $F \subset K\langle X\rangle$, the set of leading monomials of F is $\mathrm{lm}(F) \coloneqq \{\mathrm{lm}(f) \mid f \in F \setminus \{0\}\}$ and the set of leading terms of F is $\mathrm{lt}(F) \coloneqq \{\mathrm{lt}(f) \mid f \in F\}$.

2.3 Reduction

One of the most important tools in Gröbner basis theory is the reduction algorithm. It is a multivariate generalization of the classical (univariate) polynomial division with remainder. Also, instead of one polynomial, we divide by a set of polynomials.

We will keep this section close to the exposition in [Nor01a].

Definition 2.15. Let F be a subset of $K\langle X\rangle$ and let $w \in \langle X\rangle$ be a word. We say that w is *normal* modulo F if $\mathrm{lm}(f) \nmid w$ for all $f \in F$.

Definition 2.16. Let F be a subset of $K\langle X\rangle$ and let $f \in K\langle X\rangle$ be a polynomial. We say that f is *reduced* modulo F if all words in $\mathrm{supp}(f)$ are normal modulo F.

Remark. The zero polynomial does not contain any words, therefore it is by definition reduced.

In the following, Algorithm 1, Proposition 2.17 and Definition 2.18 are slightly modified versions of the formulations in [Nor01a].

Algorithm 1 Reduction

Given a polynomial $f \in K\langle X\rangle$ and a subset $F \subset K\langle X\rangle$, the *reduction* of f with F is performed as follows:

1. $p_1 \coloneqq f, \quad i = 1$
2. If p_i is reduced modulo F, return p_i and terminate.
3. Let w_i be the greatest word in $\operatorname{supp}(p_i)$ that is not normal modulo F. Let c_w be the coefficient of w_i in p_i and choose some $f_i \in F$ and $u_i, v_i \in \langle X\rangle$ with $w_i = u_i \operatorname{lm}(f_i) v_i$.
4. $p_{i+1} \coloneqq p_i - (c_w / \operatorname{lc}(f_i)) u_i f_i v_i$
5. Increment i by one and go to step 2.

Proposition 2.17. *For every finite subset $F \subset K\langle X\rangle$ and every polynomial $f \in K\langle X\rangle$, Algorithm 1 terminates and yields a representation*

$$f = \sum_{i=1}^{k} c_i u_i f_i v_i + r, \qquad \operatorname{lm}(u_i f_i v_i) \preceq \operatorname{lm}(f) \quad \forall i, \tag{2.2}$$

where $c_i \in K$, $u_i, v_i \in \langle X\rangle$, $f_i \in F$ and the remainder $r \in K\langle X\rangle$ is reduced modulo F.

Proof. We will first show that Algorithm 1 terminates. In step 4 the coefficient is chosen such that the occurrence of w_i in p_i is canceled. Because $\prec$ is a monomial ordering, the subtraction in step 4 cannot introduce new words greater than w_i. Therefore, the next time step 3 is reached, w_i must be smaller than w_{i-1}. Suppose the algorithm does not terminate. Then the words chosen each time in step 3 would give rise to an infinite descending chain of words. This is a contradiction because $\prec$ is a well-ordering.

We will now show, that the algorithm yields the representation (2.2). By keeping track of u_i, f_i, v_i and the coefficient we subtract in step 4, we get u_i, f_i, v_i and c_i respectively for (2.2). The p_i that is returned at the end of the algorithm in step 2 is used as r for (2.2). Now the first part of (2.2) obviously holds.

By the argument about the termination, it is clear that $\operatorname{lm}(p_i) \preceq \operatorname{lm}(p_{i-1})$. Also remember that $p_1 = f$. Then, because $\operatorname{lm}(u_i f_i v_i) = w_i \preceq \operatorname{lm}(p_i) \preceq \operatorname{lm}(f)$, the second part of (2.2) holds too. □

Definition 2.18. We call the element r in Proposition 2.17 a *remainder* of f modulo F and we say f *reduces* to r over F.

We say *a* remainder not without a reason. Depending on which elements f_i, u_i and v_i are chosen in step 3 of Algorithm 1, the remainder might be different.

Example 2.19. Consider $K\langle x, y\rangle$ equipped with the degree left lexicographic ordering such that $x \succ y$. Let $F = \{xx - y, xxy - y\}$ be a subset of $K\langle x, y\rangle$. If we reduce the polynomial xxx with F, we must use $xx - y$ but we have two possibilities:

1. $\underline{xx}x \xrightarrow{xx-y} yx$, or
2. $x\underline{xx} \xrightarrow{xx-y} xy$.

If we reduce the polynomial xxy with F, we have to choose between $xx - y$ and $xxy - y$:

1. $\underline{xx}y \xrightarrow{xx-y} yy$, or
2. $\underline{xxy} \xrightarrow{xxy-y} y$.

We have underlined the subword on the left-hand side that is equal to the leading word of the reductor.

The following definitions are inspired by (2.2) and will be useful in the next section.

Definition 2.20. Let $f \in K\langle X\rangle \setminus \{0\}$ be a polynomial. We say that f has a *Gröbner representation* in $F \subset K\langle X\rangle$ if there exist $c_i \in K$, $u_i, v_i \in \langle X\rangle$ and $f_i \in F \setminus \{0\}$ such that

$$f = \sum_{i=1}^{k} c_i u_i f_i v_i, \qquad \mathrm{lm}(u_i f_i v_i) \preceq \mathrm{lm}(f) \quad \forall i.$$

For convenience we also say that the zero polynomial has a Gröbner representation in F.

From Proposition 2.17 we now immediately get

Corollary 2.21. *Let F be a subset of $K\langle X\rangle$ and let $f \in K\langle X\rangle$ be a polynomial. If f reduces to zero over F, then f has a Gröbner representation in F.*

The following definition is from [Nor01a].

Definition 2.22. Let $\sum_{i=1}^{k} f_i$ be a sum of polynomials in $K\langle X\rangle$. The *height* of the sum is the leading monomial of the elements in the sum with the greatest leading monomial, that is $\max_i(\mathrm{lm}(f_i))$. The *breadth* of the sum is the number of elements in the sum whose leading monomial is equal to the height of the sum.

In this context a polynomial $f \in K\langle X\rangle \setminus \{0\}$ has a Gröbner representation in $F \subset K\langle X\rangle$ if and only if it can be represented by a sum $f = \sum_{i=1}^{k} c_i u_i f_i v_i$ of height $\mathrm{lm}(f)$ with $f_i \in F$. An important observation is that if $f = \sum_{i=1}^{t} p_i$ for some $p_i \in K\langle X\rangle$ and the height of the sum is greater than $\mathrm{lm}(f)$, then the breadth of the sum must be at least two, since all leading monomials greater than $\mathrm{lm}(f)$ cancel each other out.

Chapter 3

Gröbner Bases

Based on the work of Buchberger [Buc65, Buc85] and Bergman [Ber78], Mora generalized Gröbner bases and Buchberger's algorithm to the free associative algebra in [Mor86, Mor94]. In this chapter we give an introduction to Gröbner bases in the free associative algebra. We will focus on the most important parts and refer the interested reader to [Nor01a] where a similar chapter can be found.

Recall that a monomial ordering is assumed to be given.

Definition 3.1. Let I be an ideal of $K\langle X\rangle$ and let G be a subset of I. We say G is a *Gröbner basis* of I if the leading monomial of an arbitrary polynomial in $I \setminus \{0\}$ is divisible by the leading monomial of a polynomial in G.

Remark. For every ideal I, the set $G = I$ is a Gröbner basis of I. In practice, however, this particular Gröbner basis does not have much relevance.

What follows are the most frequently used characteristics of Gröbner bases.

Proposition 3.2. *Let I be an ideal of $K\langle X\rangle$ and let G be a subset of I. The following statements are equivalent.*

1. *G is a Gröbner basis of I.*
2. *$\mathrm{lm}(G)$ and $\mathrm{lm}(I)$ generate the same ideal.*
3. *Every polynomial $f \in I$ reduces to zero over G.*
4. *Every polynomial $f \in I$ has a Gröbner representation in G.*

Proof.

1. $\iff$ 2. Suppose G is a Gröbner basis of I. By Definition 3.1, for every $f \in I$ there exists $g \in G$ with $\mathrm{lm}(g) \mid \mathrm{lm}(f)$. Thus $\mathrm{lm}(f) \in \langle \mathrm{lm}(G)\rangle$ and $\langle \mathrm{lm}(I)\rangle \subseteq \langle \mathrm{lm}(G)\rangle$. Because $G \subseteq I$, it follows immediately that $\langle \mathrm{lm}(G)\rangle \subseteq \langle \mathrm{lm}(I)\rangle$.

Now suppose G is not a Gröbner basis of I. Then there exists $f \in I$ with $\mathrm{lm}(g) \nmid \mathrm{lm}(f)$ for all $g \in G$ and hence $\mathrm{lm}(f) \notin \langle \mathrm{lm}(G)\rangle$ and $\langle \mathrm{lm}(I)\rangle \neq \langle \mathrm{lm}(G)\rangle$.

1. $\implies$ **3.** If G is a Gröbner basis of I, then reducing f with G yields a representation $f = \sum_{i=1}^{k} c_i u_i g_i v_i + r$ with $c_i \in K$, $u_i, v_i \in \langle X \rangle$ and $g_i \in G$ where either r is equal to 0 or $\mathrm{lm}(g) \nmid \mathrm{lm}(r)$ for all $g \in G$. Because $r = f - \sum_{i=1}^{k} c_i u_i g_i v_i \in I$ and G is a Gröbner basis of I, r must be equal to 0 to avoid a contradiction with Definition 3.1.

3. $\implies$ **4.** Since f reduces to zero over G, by Corollary 2.21 f has a Gröbner representation in G.

4. $\implies$ **1.** We show the contraposition. If G is not a Gröbner basis, then there exists $f \in I \setminus \{0\}$ with $\mathrm{lm}(g) \nmid \mathrm{lm}(f)$ for all $g \in G$ and thus f has no Gröbner representation in G. □

In contrast to Gröbner bases in commutative algebras, a Gröbner basis in the free associative algebra does not necessarily have to be finite. In fact, there are ideals where no finite Gröbner basis exists, either for all or only some orderings.

Also, unlike in the commutative case, for a polynomial $f \in K\langle X \rangle$ the set $\{f\}$ is not necessarily a Gröbner basis of $\langle f \rangle$. The following is a classic example for this case.

Example 3.3. Let $g = x^2 - xy$ and consider the ideal $\langle g \rangle$ in $K\langle x, y \rangle$ with the degree left lexicographic ordering such that $x \succ y$. Clearly $f = xg - gx + gy = xyx - xyy \in \langle g \rangle$ but $\mathrm{lm}(g) \nmid \mathrm{lm}(f)$. So in this case $\{g\}$ is not a Gröbner basis of $\langle g \rangle$. With respect to this ordering, a minimal Gröbner basis of $\langle g \rangle$ is the infinite set $\{xy^i x - xy^{i+1} \mid i \in \mathbb{N}_0\}$. However, for an arbitrary monomial ordering that satisfies $xy \succ x^2$, $\{g\}$ itself is already a Gröbner basis of $\langle g \rangle$.

If G is a Gröbner basis of I, then by Proposition 3.2 every polynomial $f \in I$ reduces to zero over G and thus can be written as $f = \sum_{i=1}^{k} c_i u_i g_i v_i \in \langle G \rangle$ with $c_i \in K$, $u_i, v_i \in \langle X \rangle$ and $g_i \in G$. This leads us to

Corollary 3.4. *Let I be an ideal of $K\langle X \rangle$ and let G be a subset of I. If G is a Gröbner basis of I, then G generates I.*

Definition 3.5. Let G be a subset of $K\langle X \rangle$. We say G is a Gröbner basis if G is a Gröbner basis of $\langle G \rangle$.

3.1 Verification

While the results in this section were not initially introduced by Nordbeck, we have kept this section very close to his formulations in [Nor01a] (Section 2.2) and further elaborated the proofs of Proposition 3.6 and Theorem 3.9.

Before we actually compute Gröbner bases, let us first consider how we can verify that a set of polynomials is a Gröbner basis. Using Proposition 3.2 we have a method to verify whether a subset G of $K\langle X \rangle$ is a Gröbner basis by verifying if every polynomial in $\langle G \rangle$ reduces to zero. Unfortunately, this would take infinitely long because there are infinitely many polynomials $\langle G \rangle$ (not considering the zero ideal). In this section we aim to limit the set of polynomials that we have to consider.

If G is not a Gröbner basis, then there is at least one polynomial $f \in \langle G \rangle$ that has no Gröbner representation in G. Since $f \in \langle G \rangle$, there exists some representation

$$f = \sum_{i=1}^{k} c_i u_i g_i v_i, \quad c_i \in K,\ u_i, v_i \in \langle X \rangle,\ g_i \in G, \tag{3.1}$$

and by assumption $\operatorname{lm}(u_i g_i v_i) \succ \operatorname{lm}(f)$ for at least one i. Recall that if i is chosen such that $\operatorname{lm}(u_i g_i v_i)$ is equal to the height of the sum, then the breadth of the sum is at least two and thus there must exist at least one more index j such that $\operatorname{lm}(u_j g_j v_j) = \operatorname{lm}(u_i g_i v_i) \succ \operatorname{lm}(f)$. This leads us to pairs $g, g' \in G$ with $u \operatorname{lm}(g) v = u' \operatorname{lm}(g') v'$ for some $u, v, u', v' \in \langle X \rangle$. To be more precise:

Proposition 3.6 ([Nor01a, Proposition 5])**.** *Let G be a subset of $K\langle X \rangle$. G is a Gröbner basis if for all $g, g' \in G$ and $u, v, u', v' \in \langle X \rangle$ with $u \operatorname{lm}(g) v = u' \operatorname{lm}(g') v'$ either $ugv - \frac{\operatorname{lc}(g)}{\operatorname{lc}(g')} u' g' v' = 0$ or there exists some representation*

$$ugv - \frac{\operatorname{lc}(g)}{\operatorname{lc}(g')} u' g' v' = \sum_{i=1}^{k} c_i u_i g_i v_i, \qquad \operatorname{lm}(u_i g_i v_i) \prec \operatorname{lm}(ugv) = \operatorname{lm}(u' g' v') \quad \forall i,$$

with $c_i \in K,\ u_i, v_i \in \langle X \rangle,\ g_i \in G$.

Proof. We will show that every polynomial in $\langle G \rangle$ has a Gröbner representation in G. By Proposition 3.2 we know that this is sufficient to show that G is a Gröbner basis. Let us assume for a contradiction that there exists a polynomial $f \in \langle G \rangle$ that does not admit any Gröbner representation in G. Choose some representation of f as in (3.1) with minimal height and minimal breadth for that height. We already know that there are at least two summands with greatest leading monomial. By renumbering, we can assume that $\operatorname{lm}(u_1 g_1 v_1) = \operatorname{lm}(u_2 g_2 v_2)$. We can then rewrite the chosen representation as

$$f = \sum_{i=1}^{k} c_i u_i g_i v_i = c_1 u_1 g_1 v_1 + c_2 u_2 g_2 v_2 + \sum_{i=3}^{k} c_i u_i g_i v_i \tag{3.2}$$

$$= c_1 u_1 g_1 v_1 + c_2 u_2 g_2 v_2 + \underbrace{c_1 \frac{\operatorname{lc}(g_1)}{\operatorname{lc}(g_2)} u_2 g_2 v_2 - c_1 \frac{\operatorname{lc}(g_1)}{\operatorname{lc}(g_2)} u_2 g_2 v_2}_{0} + \sum_{i=3}^{k} c_i u_i g_i v_i \tag{3.3}$$

$$= c_1 \left(u_1 g_1 v_1 - \frac{\operatorname{lc}(g_1)}{\operatorname{lc}(g_2)} u_2 g_2 v_2 \right) + \left(c_2 + c_1 \frac{\operatorname{lc}(g_1)}{\operatorname{lc}(g_2)} \right) u_2 g_2 v_2 + \sum_{i=3}^{k} c_i u_i g_i v_i. \tag{3.4}$$

By assumption, the first term in (3.4) can be written as a sum in G with height smaller than $\operatorname{lm}(u_1 g_1 v_1)$. Therefore, if the breadth of the original sum was two and $c_2 + c_1(\operatorname{lc}(g_1)/\operatorname{lc}(g_2)) = 0$, then we can write f as a sum in G with smaller height than the original sum. Otherwise, we can write f as a sum in G with the same height but decreased breadth compared to the original sum. Both cases contradict with one of the two minimality conditions from before. □

Yet we are facing the same problem as before. We cannot directly use Proposition 3.6 to verify that G is a Gröbner basis in finitely many steps since we would have to consider infinitely many pairs. But as we will soon see, it suffices to consider the pairs where the leading monomials overlap as in the following sense.

Definition 3.7 ([Nor01a, Definition 9])**.** Let $w, w' \in \langle X \rangle$. We say that w, w' form an *overlap* if there exist $u, v \in \langle X \rangle$ such that

1. $wu = vw', \quad |u| < |w'|,\ |v| < |w|,\ u, v \neq \varepsilon,$
2. $uw = w'v, \quad |u| < |w'|,\ |v| < |w|,\ u, v \neq \varepsilon,$
3. $w = uw'v$, or
4. $uwv = w'$.

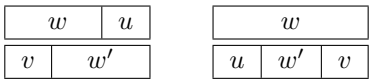


Figure 3.1: The overlaps in case 1 and 3

Remark. By possibly interchanging the meaning of w and w', it is clear that the cases 2 and 4 are already covered by the cases 1 and 3.

A pair of words can form multiple overlaps, consider for example $w = yx$ and $w' = xyx$. They form the overlaps $xw = w'$ and $wyx = yw'$. Furthermore, w' forms two overlaps with itself, namely $xyw' = w'yx$ and $w'yx = xyw'$, which are in this case identical.

The following definition is close to [Nor01a, Definition 10].

Definition 3.8. If the leading monomials of $f, f' \in K\langle X \rangle$ form an overlap, we call f, f' a *critical pair*. By possibly interchanging the meaning of f and f', the *overlap relations* of f, f' are

1. $fu - \frac{\operatorname{lc}(f)}{\operatorname{lc}(f')} vf' \quad$ for each overlap $\operatorname{lm}(f)u = v \operatorname{lm}(f')$, and
2. $f - \frac{\operatorname{lc}(f)}{\operatorname{lc}(f')} uf'v \quad$ for each overlap $\operatorname{lm}(f) = u \operatorname{lm}(f')v$.

The coefficient $\operatorname{lc}(f)/\operatorname{lc}(f')$ is chosen such that the leading monomials of the two terms cancel each other out. Therefore, if the overlap relation is not equal to zero, the leading monomial of the overlap relation is smaller than the two monomials forming the overlap.

We have further elaborated the proof of [Nor01a, Proposition 6] to prove the following theorem.

Theorem 3.9. *Let G be a subset of $K\langle X \rangle$. G is a Gröbner basis if and only if each overlap relation of every critical pair in G has a Gröbner representation in G.*

Proof. First, assume G is a Gröbner basis. We already know that every polynomial in $\langle G\rangle$ has a Gröbner representation in G. Clearly each overlap relation of every critical pair in G lies in $\langle G\rangle$.

Assume conversely that each overlap relation of every critical pair in G has a Gröbner representation in G. We will use Proposition 3.6, therefore let $g, g' \in G$ and $u, v, u', v' \in \langle X\rangle$ such that $u\,\mathrm{lm}(g)v = u'\,\mathrm{lm}(g')v'$. We need to show that $f = ugv - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}u'g'v'$ has a representation as in Proposition 3.6. If f is equal to zero, we are already done. Therefore assume f is not equal to zero. By removing variables from the left- and right-hand side of the equality $u\,\mathrm{lm}(g)v = u'\,\mathrm{lm}(g')v'$ and possibly interchanging the meaning of g and g' we can achieve one of the following cases:

1. $\mathrm{lm}(g) = w\,\mathrm{lm}(g')w'$, or

2. $\mathrm{lm}(g)w = w'\,\mathrm{lm}(g')$

with $w, w' \in \langle X\rangle$. In case 1 g, g' is a critical pair. By assumption, the corresponding overlap relation has a Gröbner representation in G. Consider some Gröbner representation

$$g - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}wg'w' = \sum_{i=1}^{k} c_i u_i g_i v_i, \quad c_i \in K,\ u_i, v_i \in \langle X\rangle,\ g_i \in G \tag{3.5}$$

of the overlap relation. Then

$$\mathrm{lm}(u_i g_i v_i) \preceq \mathrm{lm}(g - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}wg'w') \prec \mathrm{lm}(g) \quad \forall i.$$

Multiplying (3.5) by u and v (the words we removed before) from the left- and right-hand side respectively, it follows that

$$\mathrm{lm}(uu_i g_i v_i v) \preceq \mathrm{lm}(ugv - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}uwg'w'v) \prec \mathrm{lm}(ugv) \quad \forall i.$$

Therefore $f = \sum_{i=1}^{k} c_i u u_i g_i v_i v$ is a representation of f as in Proposition 3.6 and we are done.

Now consider case 2. If $\mathrm{lm}(g)w = w'\,\mathrm{lm}(g')$ is an overlap, the same argument as in case one holds, we just multiply with u and v' instead of u and v respectively. Otherwise $w = \tilde{w}\,\mathrm{lm}(g')$ and $w' = \mathrm{lm}(g)\tilde{w}$ with $\tilde{w} \in \langle X\rangle$. Let $\bar{g}$

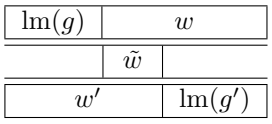


Figure 3.2: $\tilde{w}$

denote the *tail* of g, that is $g - \mathrm{lt}(g)$. It holds that

$$\begin{aligned} gw - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')} w'g' &= g\tilde{w}\,\mathrm{lm}(g') - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}\,\mathrm{lm}(g)\tilde{w}g' \\ &= g\tilde{w}\,\mathrm{lc}(g')^{-1}\underbrace{(g' - \bar{g}')}_{\mathrm{lt}(g')} - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}\,\mathrm{lc}(g)^{-1}\underbrace{(g - \bar{g})}_{\mathrm{lt}(g)}\tilde{w}g' \\ &= \underbrace{\left(\mathrm{lc}(g')^{-1} - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}\,\mathrm{lc}(g)^{-1}\right)}_{0} g\tilde{w}g' \\ &\qquad - \mathrm{lc}(g')^{-1} g\tilde{w}\bar{g}' + \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')}\,\mathrm{lc}(g)^{-1}\bar{g}\tilde{w}g' \\ &= -\mathrm{lc}(g')^{-1} g\tilde{w}\bar{g}' + \mathrm{lc}(g')^{-1}\bar{g}\tilde{w}g'. \end{aligned}$$

Clearly $\tilde{w}\,\mathrm{lm}(\bar{g}') \prec \tilde{w}\,\mathrm{lm}(g') = w$ and $\mathrm{lm}(\bar{g})\tilde{w} \prec \mathrm{lm}(g)\tilde{w} = w'$. By multiplying

$$gw - \frac{\mathrm{lc}(g)}{\mathrm{lc}(g')} w'g' = -\mathrm{lc}(g')^{-1} g\tilde{w}\bar{g}' + \mathrm{lc}(g')^{-1}\bar{g}\tilde{w}g'$$

with u and v' (the words we removed before) from the left and right side respectively, we get the representation

$$f = -\mathrm{lc}(g')^{-1} ug\tilde{w}\bar{g}'v' + \mathrm{lc}(g')^{-1} u\bar{g}\tilde{w}g'v'$$

of f with $\mathrm{lm}(ug\tilde{w}\bar{g}'v') \prec \mathrm{lm}(ugwv') = \mathrm{lm}(ugv)$ and $\mathrm{lm}(u\bar{g}\tilde{w}g'v') \prec \mathrm{lm}(uw'g'v') = \mathrm{lm}(u'g'v') = \mathrm{lm}(ugv)$ as in Proposition 3.6. □

By Corollary 2.21 and Proposition 3.2, the following proposition is an immediate result of the last theorem (it is also stated in [Nor01a, Proposition 7]).

Proposition 3.10. *Let G be a subset of $K\langle X\rangle$. G is a Gröbner basis if and only if each overlap relation of every critical pair in G reduces to zero over G.*

This leads us to our goal for this section. If the set $G \subset K\langle X\rangle$ is finite, then there can only be finitely many overlap relations among the leading monomials of the elements in G and we can verify in finitely many steps whether G is a Gröbner basis. Furthermore, if G is not a Gröbner basis, we can find an overlap relation of a critical pair in G that does not reduce to zero over G.

3.2 Computation

With the result from the last section (Proposition 3.10) in mind, we obtain an algorithm to transform a set of polynomials $F \subset K\langle X\rangle$ into a Gröbner basis of $\langle F\rangle$. First we compute each overlap relation of every critical pair in F and then reduce them with F. If an overlap relation does not reduce to zero over F, we add the remainder to F. Now each overlap relation from the original set F reduces to zero over the new set F. But new overlap relations might arise from the new set F. Therefore, we repeat the procedure until there are no new remainders left to be added.

What we have just described is basically a generalization of Buchberger's algorithm to the free associative algebra. We have slightly reformulated the algorithm as it is presented in [Nor01a, Algorithm 2].

Algorithm 2 The Gröbner basis algorithm

Given a set of polynomials $F \subset K\langle X\rangle$, we can transform F into a Gröbner basis of $\langle F\rangle$ as follows:

1. $G_1 \coloneqq F, \quad i = 1$
2. Let P_i be the set of all overlap relations in G_i.
3. $G_{i+1} \coloneqq G_i \cup \{r \mid r \text{ is a nonzero remainder of } p \in P_i \text{ modulo } G_i\}$
4. If $G_{i+1} \neq G_i$, increment i by one and go to step 2.
5. Return $G_\infty \coloneqq \bigcup G_i$.

As we have already seen before, even if $F \subset K\langle X\rangle$ is finite, there does not necessarily exist a finite Gröbner basis of $\langle F\rangle$ and therefore the algorithm might not terminate. Nonetheless, we can still prove that G_∞ is a Gröbner basis of $\langle F\rangle$.

Proposition 3.11 ([Nor01a, Proposition 8])**.** *Given a set of polynomials $F \subset K\langle X\rangle$ as input, the set G_∞ generated by Algorithm 2 is a Gröbner basis of $\langle F\rangle$.*

Proof. Because $F \subset G_\infty$ and all remainders added in step 3 are in $\langle F\rangle$, we have $\langle G_\infty\rangle = \langle F\rangle$. It remains to show that G_∞ is a Gröbner basis.

If $G_i = G_{i+1}$ for some i, then clearly all overlap relations in G_i reduce to zero over G_i and thus by Proposition 3.10 $G_i = G_\infty$ is a Gröbner basis. Otherwise, consider an arbitrary critical pair $g, g' \in G_\infty$. We know that $g \in G_i$ and $g' \in G_j$ for some i, j. Let $k = \max(i, j)$, then clearly every overlap relation of g, g' reduces to zero over $G_{k+1} \subset G_\infty$ and thus, again by Proposition 3.10, G_∞ is a Gröbner basis. □

Furthermore, we can prove that if the set F in Algorithm 2 is finite and there exists a finite Gröbner basis of $\langle F\rangle$ (with respect to the given ordering), then the algorithm terminates.

Proposition 3.12 ([Nor01a, Proposition 9])**.** *Let $F \subset K\langle X\rangle$ be a finite set of polynomials. If there exists a finite Gröbner basis of $\langle F\rangle$, then Algorithm 2 terminates with F as input.*

Proof. Let $G = \{g_1, \ldots, g_n\}$ be a finite Gröbner basis of $\langle F\rangle$. We have already seen that G_∞ is a Gröbner basis of $\langle F\rangle$. Therefore, for every element $g_i \in G \subset \langle F\rangle$ there is an element $g_i' \in G_\infty$ such that $\mathrm{lm}(g_i') \mid \mathrm{lm}(g_i)$. But then, by Definition 3.1, $\{g_1', \ldots, g_n'\}$ is also a Gröbner basis of $\langle F\rangle$. We know that every $g_i' \in G_{j_i}$ for some j_i. Let $k = \max\{j_1, \ldots, j_n\}$, then G_k is clearly a Gröbner basis and thus $G_k = G_{k+1}$. □

3.3 Applications

As we have seen in Proposition 3.2, if G is a Gröbner basis, every polynomial $f \in \langle G \rangle$ reduces to zero over G. The other way around, if a polynomial f reduces to zero over G, then obviously $f \in \langle G \rangle$. This means that we can solve the *ideal membership problem*.

Proposition 3.13. *Let I be an ideal of $K\langle X \rangle$, let G be a Gröbner basis of I and let $f \in K\langle X \rangle$ be a polynomial. f is in I if and only if f reduces to zero over G.*

Particularly, given a finite Gröbner basis of I, the reduction algorithm terminates and thus gives us a method to solve the ideal membership problem in finitely many steps.

We have further elaborated the proof of [Nor01a, Proposition 11] to prove the following proposition.

Proposition 3.14. *Let I be an ideal of $K\langle X \rangle$ and let G be a Gröbner basis of I. The remainder of the reduction of $f \in K\langle X \rangle$ with G is uniquely determined.*

Proof. Suppose two different reductions of $f \in K\langle X \rangle$ with G yield two different remainders $r, r' \in K\langle X \rangle$. That is

$$f = \sum_{i=1}^{k} c_i u_i g_i v_i + r \quad \text{and} \quad f = \sum_{i=1}^{k'} c'_i u'_i g'_i v'_i + r',$$

with $c_i, c'_i \in K$, $u_i, v_i, u'_i, v'_i \in \langle X \rangle$ and $g_i, g'_i \in G$. Then we have

$$\begin{aligned} \sum_{i=1}^{k} c_i u_i g_i v_i + r &= \sum_{i=1}^{k'} c'_i u'_i g'_i v'_i + r' \\ r - r' &= \sum_{i=1}^{k'} c'_i u'_i g'_i v'_i - \sum_{i=1}^{k} c_i u_i g_i v_i \in \langle G \rangle. \end{aligned}$$

By Proposition 2.17, r and r' are reduced modulo G, that is every word in $\mathrm{supp}(r)$ and $\mathrm{supp}(r')$ is normal modulo G. Since $\mathrm{supp}(r - r') \subseteq \mathrm{supp}(r) \cup \mathrm{supp}(r')$, it follows that every word in $\mathrm{supp}(r - r')$ is normal modulo G. Suppose $\mathrm{supp}(r - r') \neq \emptyset$, then $\mathrm{lm}(r - r')$ is normal modulo G which is a contradiction since G is a Gröbner basis and $r - r' \in \langle G \rangle$. Therefore, the only possibility is that $\mathrm{supp}(r - r') = \emptyset$ which is only the case if $r - r' = 0$ or in other words if $r = r'$. □

In fact, the ability to provide unique remainders is already characterizing for Gröbner bases. For a proof we refer the reader to page 50 of [Alu06].

We know now that for a Gröbner basis $G \subset K\langle X \rangle$ and a polynomial $f \in K\langle X \rangle$ the remainder r of f modulo G is uniquely determined. By the definition of a Gröbner basis, since r is reduced modulo G, r is also reduced modulo $I = \langle G \rangle$. Remember that we assume a fixed monomial ordering. The proof of Proposition 3.14 shows us that even if we use two different Gröbner bases of I for the reduction of f, the remainder r is still unique and further r is the unique polynomial that is reduced modulo I such that $f - r \in I$.

Definition 3.15. Let I be an ideal of $K\langle X\rangle$ and let $f \in K\langle X\rangle$ be a polynomial. The *normal form* of f modulo I, denoted by $\mathrm{nf}_I(f)$, is the unique polynomial $r \in K\langle X\rangle$ that is reduced modulo I such that $f - r \in I$.

Corollary 3.16. *Let I be an ideal of $K\langle X\rangle$, let G be a Gröbner basis of I and let $f \in K\langle X\rangle$ be a polynomial. The remainder of the reduction of f with G is the normal form of f modulo I.*

Obviously we can now simplify Proposition 3.13, we have $f \in I$ if and only if $\mathrm{nf}_I(f) = 0$.

The normal form plays an important role when we want to work in the factor algebra $K\langle X\rangle/I$. Let us investigate when two elements $f + I$, $f' + I \in K\langle X\rangle/I$ are equal. The following holds

$$\begin{aligned} & f + I = f' + I \\ \iff \quad & (f + I) - (f' + I) = 0 \\ \iff \quad & f - f' + I = 0 \\ \iff \quad & f - f' \in I \\ \iff \quad & \mathrm{nf}_I(f - f') = 0. \end{aligned}$$

Lemma 3.17. *Let I be an ideal of $K\langle X\rangle$ and let $f, f' \in K\langle X\rangle$ be two polynomials. Then $\mathrm{nf}_I(f - f') = 0$ if and only if $\mathrm{nf}_I(f) = \mathrm{nf}_I(f')$.*

Proof. Suppose $\mathrm{nf}_I(f - f') = 0$, that is $f - f' \in I$. We always have some representations $f = g + r$ and $f' = g' + r'$ with $g, g' \in I$, $r, r' \in K\langle X\rangle$ and r, r' reduced modulo I. Then $f - f' = g + r - (g' - r') = (g - g') + (r - r') \in I$ and since $g - g' \in I$ we have $r - r' \in I$. Now the only possibility is that $r - r' = 0$ and thus $r = r'$ giving us $\mathrm{nf}_I(f) = \mathrm{nf}_I(f')$.

The other way around, suppose $\mathrm{nf}_I(f) = \mathrm{nf}_I(f')$. Then we have some representations $f = g + r$ and $f' = g' + r$ with $g, g' \in I$, $r \in K\langle X\rangle$ and r reduced modulo I. It follows that $f - f' = g + r - (g' - r) = (g - g') \in I$ and thus $\mathrm{nf}_I(f - f') = 0$. □

Combining the results, we get

Proposition 3.18. *Two elements $f + I$, $f' + I \in K\langle X\rangle/I$ are equal if and only if $\mathrm{nf}_I(f) = \mathrm{nf}_I(f')$.*

It follows that a set of representatives of the elements of $K\langle X\rangle/I$ is given by $\{\mathrm{nf}_I(f) \mid f \in K\langle X\rangle\}$. Recall from Definition 2.15 that a word $w \in \langle X\rangle$ is said to be normal modulo I if $\mathrm{lm}(f) \nmid w$ for all $f \in I$. Consider the set $N = \{w \mid w \in \langle X\rangle \text{ is normal modulo } I\}$ of all words that are normal modulo I. N is a subset of $\langle X\rangle$ and therefore N generates the vector subspace KN of $K\langle X\rangle$ and is further a K-basis of KN. Since $\mathrm{nf}_I(f)$ is reduced modulo I, clearly $\mathrm{supp}(\mathrm{nf}_I(f)) \subset N$ and thus $\mathrm{nf}_I(f) \in KN$ for all $f \in K\langle X\rangle$. Conversely, for $f \in KN$ we have that f is reduced modulo I, that is $f = \mathrm{nf}_I(f)$. It follows that $KN = \{\mathrm{nf}_I(f) \mid f \in K\langle X\rangle\}$ and thus KN is isomorphic to $K\langle X\rangle/I$ as a vector space. An isomorphism is given by $KN \to K\langle X\rangle/I$, $f \mapsto f + I$. Summarizing, we get

Proposition 3.19. *Let I be an ideal of $K\langle X\rangle$ and N the set of all words normal modulo I. The vector subspace KN of $K\langle X\rangle$ is isomorphic to $K\langle X\rangle/I$ as a vector space and N is a K-basis of KN.*

Since clearly the set of all words normal modulo I is the same as the set of all words normal modulo $\langle \operatorname{lm}(I)\rangle$, we also get

Proposition 3.20. *Let I be an ideal of $K\langle X\rangle$. Then $K\langle X\rangle/I$ and $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ are isomorphic as vector spaces.*

3.4 Reduced Gröbner Bases

Definition 3.21. Let $F \subset K\langle X\rangle$ be a set of polynomials. We say F is *reduced* if the following conditions hold for all $f \in F$.

1. f is reduced modulo $F \setminus \{f\}$.
2. f is monic, that is $\operatorname{lc}(f) = 1$.

Remark. A Gröbner basis is a set of polynomials, therefore Definition 3.21 also applies to Gröbner bases.

For the proof of the following theorem, we have reused a part of the "Uniqueness" part in the proof of [Alu06, Theorem 3.3.2].

Theorem 3.22. *Let $G \subset K\langle X\rangle$ be a finite Gröbner basis. There exists a unique reduced Gröbner basis G' of $\langle G\rangle$.*

Proof.

Existence We claim that

$$G' = \{\operatorname{lc}(r)^{-1} r \mid r \text{ is the remainder of } g \in G \text{ modulo } G \setminus \{g\} \text{ and } r \neq 0\}$$

is a reduced Gröbner basis of $\langle G\rangle$. Since G is finite, we can compute G' in finitely many steps. Obviously G' satisfies the conditions of a reduced set as in Definition 3.21. We will now show that G' is in fact a Gröbner basis of $\langle G\rangle$. Clearly G' is a subset of $\langle G\rangle$ and for all $g \in G$ there exists $g' \in G'$ with $\operatorname{lm}(g') \mid \operatorname{lm}(g)$. For each $f \in \langle G\rangle$ there exists $g \in G$ with $\operatorname{lm}(g) \mid \operatorname{lm}(f)$ and therefore there exists $g' \in G'$ with $\operatorname{lm}(g') \mid \operatorname{lm}(g) \mid \operatorname{lm}(f)$. Thus G' is by definition a Gröbner basis of $\langle G\rangle$.

Uniqueness Let us assume for a contradiction that there are two reduced Gröbner bases G and H generating the same ideal. First, choose an element $g \in G$. Because g lies in $\langle H\rangle$, there must be a polynomial $h \in H$ such that $\operatorname{lm}(h) \mid \operatorname{lm}(g)$. Conversely, because h lies in $\langle G\rangle$ there must exist a polynomial $g' \in G$ such that $\operatorname{lm}(g') \mid \operatorname{lm}(h)$. This implies that $\operatorname{lm}(g') \mid \operatorname{lm}(g)$ but because G is reduced that means $\operatorname{lm}(g') = \operatorname{lm}(g)$. Because $\operatorname{lm}(h) \mid \operatorname{lm}(g)$ and $\operatorname{lm}(g) \mid \operatorname{lm}(h)$, the only possibility is $\operatorname{lm}(h) = \operatorname{lm}(g)$. We have shown that for each element $g \in G$ there exists an element $h \in H$ with $\operatorname{lm}(g) = \operatorname{lm}(h)$. The same argument goes the other way around and therefore $\operatorname{lm}(G) = \operatorname{lm}(H)$.

We yet have to show that $\operatorname{lm}(g) = \operatorname{lm}(h)$ implies $g = h$. For a contradiction we assume that $g \neq h$. Consider the polynomial $g - h$. Without loss of generality assume $\operatorname{lm}(g-h) \in \operatorname{supp}(g)$. Now, because $g - h$ lies in $\langle G\rangle$ there must be $g' \in G$ such that $\operatorname{lm}(g') \mid \operatorname{lm}(g - h)$. This is a contradiction because $\operatorname{lm}(g')$ divides a word in $\operatorname{supp}(g)$ but G is reduced. □

Observation 3.23. Let G be a Gröbner basis and $g, g' \in G$. If $\mathrm{lm}(g) \mid \mathrm{lm}(g')$, then g' reduces to zero over $G \setminus \{g'\}$.

Proof. Consider the first step of the reduction, that is $g'' = g' - \frac{\mathrm{lc}(g')}{\mathrm{lc}(g)} g$. Clearly $g'' \in \langle G \rangle$, so g'' reduces to zero over G. If g'' is not equal to zero, then since $\mathrm{lm}(g'') \prec \mathrm{lm}(g')$ we also have that g'' reduces to zero over $G \setminus \{g'\}$. It follows that g' reduces to zero over $G \setminus \{g'\}$. □

3.5 Homogeneous Gröbner Bases

Definition 3.24. Let $f \in K\langle X \rangle$ be a polynomial. We say f is homogeneous if all words in $\mathrm{supp}(f)$ have the same length.

Furthermore, we say that a set of polynomials $F \subset K\langle X \rangle$ homogeneous if every polynomial in the set is homogeneous. For an ideal $I \subset K\langle X \rangle$, we say that I is homogeneous if there exists a homogeneous set that generates I.

Keep in mind that if we add two homogeneous polynomials of the same degree, then the result is either the zero polynomial or a homogeneous polynomial of the same degree. Multiplying a homogeneous polynomial f with a word w results in a homogeneous polynomial of degree $\deg(f) + |w|$. Now the following is easy to see.

Lemma 3.25. *Let $f \in K\langle X \rangle$ be a homogeneous polynomial and let $F \subset K\langle X \rangle$ be a homogeneous set. The remainder r of the reduction of f with F (as in Algorithm 1) is homogeneous and either $r = 0$ or $\deg(r) = \deg(f)$.*

Clearly, possible overlap relations of two homogeneous polynomials are also homogeneous. Then with the same argument we get

Lemma 3.26. *Let $F \subset K\langle X \rangle$ be a homogeneous set. The Gröbner basis generated by Algorithm 2 is homogeneous.*

It follows

Lemma 3.27. *Let I be a homogeneous ideal of $K\langle X \rangle$. The reduced Gröbner basis of I is homogeneous.*

Proof. If I is a homogeneous ideal, then there exists a homogeneous set $F \subset I$ that generates I. By Lemma 3.26, there exists a homogeneous Gröbner basis G of $\langle F \rangle = I$. Looking at the approach in the proof of Theorem 3.22 to construct the unique reduced Gröbner basis G' of I from G, it is clear that G' is also homogeneous. □

Lemma 3.28. *Let a homogeneous set be the input for Algorithm 2. If the polynomial of smallest degree in $G_{i+1} \setminus G_i$ of Algorithm 2 has degree k, then all polynomials in $G_{i+2} \setminus G_{i+1}$ have at least degree k.*

Proof. We use the notation from Algorithm 2. Assume the polynomial of smallest degree in $G_{i+1} \setminus G_i$ has degree k and consider some arbitrary polynomial $r \in G_{i+2} \setminus G_{i+1}$. Then $r \neq 0$ is the remainder of some $p \in P_{i+1}$ modulo G_{i+1}. Clearly all polynomials in P_i reduce to zero over G_{i+1} and thus $p \in P_{i+1} \setminus P_i$. It follows that p is an overlap relation of some pair f, f' with $f \in G_{i+1}$ and

$f' \in G_{i+1} \setminus G_i$. By assumption, the polynomial of smallest degree in $G_{i+1} \setminus G_i$ has degree k and therefore the degree of f' is at least k which means the degree of p is at least k. Then by Lemma 3.25, the degree of r is at least k. □

Theorem 3.29. *Let $F \subset K\langle X\rangle$ be a finite homogeneous set, G_∞ the possibly infinite Gröbner basis of $\langle F\rangle$ generated by Algorithm 2 and $k \in \mathbb{N}$. We can compute the set $G^{(k)} = \{g \in G_\infty \mid \deg(g) \leq k\}$ in finitely many steps.*

Proof. Since there are only finitely many polynomials of degree less than k, by Lemma 3.28, Algorithm 2 computes all polynomials in $G^{(k)}$ after finitely many rounds. □

It is clear that if we reduce a polynomial $f \in K\langle X\rangle$ of degree k over a homogeneous set $G \subset K\langle X\rangle$, then no polynomial in G of degree greater than k needs to be considered for the reduction. Consider the set $G^{(k)} \subset G_\infty$ from Theorem 3.29. Since $G^{(k)}$ is homogeneous, the reduction of f with $G^{(k)}$ yields the same result as the reduction of f with G_∞. By Theorem 3.29, we can compute $G^{(k)}$ in finitely many steps. It follows that, given a homogeneous set of generators, we can in fact solve the ideal membership problem for homogeneous ideals in finitely many steps.

3.6 Right Factor-Gröbner Bases

Now that the reader has the basic knowledge about Gröbner bases we will discuss a rather special case. We will give a definition for Gröbner bases of right ideals in factor algebras and develop a way to compute them. This section is close to the exposition in [Nor01b] (Section 6.2).

Until the end of this section let I be a (two-sided) ideal of $K\langle X\rangle$ that we are going to factor out. We will be working in the factor algebra $K\langle X\rangle/I$ and thus the normal form in this section will always be with respect to I.

Definition 3.30. For a right ideal J of $K\langle X\rangle$ we denote with $\bar{J}$ the image of J in $K\langle X\rangle/I$, that is $\bar{J} = \{f + I \mid f \in J\}$.

Remark. Since $\mathrm{nf}_I(f)$ is a unique representative of the image of $f \in J$ in $K\langle X\rangle/I$, we can *think of* $\bar{J}$ as $\{\mathrm{nf}_I(f) \mid f \in J\}$. In reality $\bar{J}$ is just defined as the image of J in $K\langle X\rangle/I$ and $\mathrm{nf}_I(f)$ is just one possible representative of the image of f.

The following observation is essential for the definition of right Factor-Gröbner bases.

Proposition 3.31. *There is a one-to-one correspondence between right ideals of $K\langle X\rangle$ containing I and right ideals of $K\langle X\rangle/I$.*

Proof. For a right ideal $J \supseteq I$ of $K\langle X\rangle$ consider the image $\bar{J}$ of J in $K\langle X\rangle/I$. It is easy to verify that $\bar{J}$ is a right ideal of $K\langle X\rangle/I$. The other way around for a right ideal J' of $K\langle X\rangle/I$ we get the set $J = \{f + g \mid f \in J',\ g \in I\} \supseteq I$. Again it is easy to verify that J is a right ideal of $K\langle X\rangle$ and we also immediately see that $\bar{J} = J'$. □

Definition 3.32 ([Nor01b, Definition 12])**.** Let $\bar{J}$ be a right ideal of $K\langle X\rangle/I$, meaning that J is a right ideal of $K\langle X\rangle$ containing I. We call a set of normal elements $F \subset J$ a *right Factor-Gröbner basis* of $\bar{J}$, or shorter a *right FG-basis* of $\bar{J}$, if for all polynomials $f \in J$ with $\mathrm{nf}_I(f) \neq 0$ there exists a polynomial $f_i \in F$ such that $\mathrm{lm}(f_i)$ is a left subword of $\mathrm{lm}(\mathrm{nf}_I(f))$.

Remark. Of course, working with left ideals instead of right ideals is completely symmetrical and in fact it would be a more classical way to define one-sided Gröbner bases in terms of left ideals. The reason we still chose to work with right ideals, is that for the way we implemented the algorithms, it is much easier to work with right ideals. This will become clear in Section 4.3.

For convenience we say that the right ideal generated by $F \subset K\langle X\rangle$ in $K\langle X\rangle/I$ is the right ideal generated by $\{f + I \mid f \in F\} \subset K\langle X\rangle/I$. Consider the right ideal $\bar{J}$ of $K\langle X\rangle/I$ generated by a set of normal elements $F \subset K\langle X\rangle$ and let G be a Gröbner basis of I. Clearly, every element $f \in J$, in particular $\mathrm{nf}_I(f)$, has a representation

$$f = \sum_{i=1}^{k} c_i f_i w_i + \sum_{j=1}^{t} c'_j u_j g_j v_j \tag{3.6}$$

with $c_i, c'_j \in K$, $f_i \in F$, $g_j \in G$ and $w_i, u_j, v_j \in \langle X\rangle$. The other way around, every element that has a representation as in (3.6) is in J. One might think that if f is normal, then the second sum on the right-hand side of (3.6) must be zero. But almost the opposite is true, even though f_i is normal, $f_i w_i$ does not have to be normal and thus for f to be normal it might even be necessary to introduce elements from G into the sum. With the notation as before, consider for example $f = f_i w_i$ and assume f is not normal, then by computing the normal form of f we get $\mathrm{nf}_I(f) = f_i w_i + \sum_{j=1}^{k} c'_j u_j g_j v_j$.

It should be clear now that for defining a reduction procedure we need to consider both F and G since even though when we reduce a normal element with another normal element, the result might not be normal.

Algorithm 3 ([Nor01b]) Right FG-reduction

Given a polynomial $f \in K\langle X\rangle$ and a subset $F \subset K\langle X\rangle$, the *right FG-reduction* in $K\langle X\rangle/I$ of f with F is performed as follows:

1. $p_1 \coloneqq f, \quad i = 1$
2. $p'_i \coloneqq \mathrm{nf}_I(p_i)$ (with respect to I).
3. If $p'_i = 0$ or if there is no $f_i \in F$ such that $\mathrm{lm}(f_i)$ is a left subword of $\mathrm{lm}(p'_i)$, return p'_i and terminate.
4. Choose some $f_i \in F$ and $w_i \in \langle X\rangle$ with $\mathrm{lm}(p'_i) = \mathrm{lm}(f_i)w_i$.
5. $p_{i+1} \coloneqq p'_i - \frac{\mathrm{lc}(p'_i)}{\mathrm{lc}(f_i)} f_i w_i$
6. Increment i by one and go to step 2.

It is easy to see that the right FG-reduction does not differ much from the normal reduction. In the normal reduction we just reduce with F and in the

right FG-reduction we reduce with a Gröbner basis of I and also (but only using right multiples) with F. Unsurprisingly, we get similar results as earlier with the normal reduction. For example, since $p_{i+1} \prec p'_i \preceq p_i$ it follows that the right FG-reduction terminates.

Proposition 3.33 ([Nor01b, Proposition 7])**.** *Let $\bar{J}$ be the right ideal of $K\langle X\rangle/I$ generated by $F \subset K\langle X\rangle$. If F is a right FG-basis, then an element $f \in K\langle X\rangle$ is in J if and only if f right FG-reduces to zero over F.*

Proof. If f right FG-reduces to zero over F, then the reduction yields a representation of f as in (3.6) and thus $f \in J$. The other way around, if f is in J, then using Definition 3.32 it is easy to see that the only possible option for termination in step 3 of Algorithm 3 is that the result is zero. □

As earlier in Section 3.1, in preparation to compute right FG-bases let us first analyze how we can verify that a subset $F \subset K\langle X\rangle$ is a right FG-basis of the right ideal $\bar{J} \subset K\langle X\rangle/I$ generated by F. Basically, we follow the same approach as in Section 3.1, therefore we skip most of the details. The important part will be to identify the critical pairs that we have to consider.

We need for an arbitrary element $f \in J$ with $\mathrm{nf}_I(f) \neq 0$ that $\mathrm{lm}(f_i)$ is a left subword of $\mathrm{lm}(\mathrm{nf}_I(f))$ for some $f_i \in F$. Let us have a closer look at $\mathrm{nf}_I(f)$. We already know that there is some representation

$$\mathrm{nf}_I(f) = \underbrace{\sum_{i=1}^{k} c_i f_i w_i}_{\Sigma_1} + \underbrace{\sum_{j=1}^{t} c'_j u_j g_j v_j}_{\Sigma_2} \tag{3.7}$$

with the notation as in (3.6). We want a representation of $\mathrm{nf}_I(f)$ such that $\mathrm{lm}(\mathrm{nf}_I(f)) = \max_i(\mathrm{lm}(f_i w_i))$, because then $\mathrm{lm}(f_i)$ is a left subword of $\mathrm{lm}(\mathrm{nf}_I(f))$ as required. Therefore let us check where $\mathrm{lm}(\mathrm{nf}_I(f))$ appears in the right-hand side of (3.7). One possibility is that $\mathrm{lm}(\mathrm{nf}_I(f)) = \mathrm{lm}(\Sigma_1)$, then we need that $\mathrm{lm}(\Sigma_1) = \max_i(\mathrm{lm}(f_i w_i))$. Thus, as usual in Gröbner basis theory, we have to consider the critical pairs $f_i, f_j \in F$ with $\mathrm{lm}(f_i) = \mathrm{lm}(f_j)w$ for some $w \in \langle X\rangle$ to prevent cancellation of leading monomials. Because G is a Gröbner basis, we can assume that there is no cancellation of leading monomials greater than $\mathrm{lm}(\Sigma_2)$ in Σ_2, meaning that we can assume that $\mathrm{lm}(\Sigma_2) = \max_j(\mathrm{lm}(u_j g_j v_j))$. Therefore, since $\mathrm{nf}_I(f)$ is normal modulo G, we cannot have $\mathrm{lm}(\mathrm{nf}_I(f)) = \mathrm{lm}(\Sigma_2)$. There is one case left to check, that is if $\mathrm{lm}(\mathrm{nf}_I(f))$ is neither $\mathrm{lm}(\Sigma_1)$ nor $\mathrm{lm}(\Sigma_2)$. Then the leading monomials of Σ_1 and Σ_2 must cancel each other out, meaning that we have $\mathrm{lm}(f_i w_i) = \mathrm{lm}(u_j g_j v_j)$ for some i, j. Because g_j does not divide f_i, we can cancel v_j from the right side. This leads us to the critical pairs f_i, g_j where $f_i w = u g_j$ for some $w, u \in \langle X\rangle$ with $w \prec g_j$.

To summarize this, we want all overlap relations in $F \cup G$, while elements from F can only be multiplied from the right. Since G is a Gröbner basis, it already contains the overlap relations of G. Now F needs to account for the overlap relations in F and the overlap relations between F and G.

With the prior in mind, the following proposition can be proven in a similar way as Theorem 3.9.

Proposition 3.34 ([Nor01b, Proposition 8])**.** *Let G be a Gröbner basis of an ideal I in $K\langle X\rangle$ and let F be a set of polynomials normal modulo G in $K\langle X\rangle$.*

For all $f_i, f_j \in F$ with $\mathrm{lm}(f_i) = \mathrm{lm}(f_j)w$ for some $w \in \langle X \rangle$, let P be the set of all overlap relations $p_{i,j} = f_i - \frac{\mathrm{lc}(f_i)}{\mathrm{lc}(f_j)} f_j w$. And for all $f_i \in F$, $g_j \in G$ with $\mathrm{lm}(f_i)u = v\,\mathrm{lm}(g_j)$ for some $u, v \in \langle X \rangle$, let Q be the set of all overlap relations $q_{i,j} = f_i w - \frac{\mathrm{lc}(f_i)}{\mathrm{lc}(g_j)} u g_j$. Then F is a right FG-basis of the right ideal in $K\langle X \rangle / I$ generated by F if and only if every polynomial in $P \cup Q$ right FG-reduces to zero over F.

If G and F are assumed to be finite in the last proposition, only finitely many overlap relations can arise from them and thus $P \cup Q$ is finite too. In this case we have characterized right FG-bases in terms of finitely many elements.

We are now proposed with an algorithm to compute right FG-bases.

Algorithm 4 ([Nor01b]) The right FG-basis algorithm

Let G be a Gröbner basis of an ideal I in $K\langle X \rangle$ and let F be a subset of $K\langle X \rangle$.

1. $F_1 \coloneqq \{\mathrm{nf}_I(f) \mid f \in F\}, \quad k = 1$
2. For all $f_i, f_j \in F_k$ with $\mathrm{lm}(f_i) = \mathrm{lm}(f_j)w$ for some $w \in \langle X \rangle$, let P_k be the set of all overlap relations $p_{i,j} = f_i - \frac{\mathrm{lc}(f_i)}{\mathrm{lc}(f_j)} f_j w$.
3. For all $f_i \in F_k$, $g_j \in G$ with $\mathrm{lm}(f_i)u = v\,\mathrm{lm}(g_j)$ for some $u, v \in \langle X \rangle$, let Q_k be the set of all overlap relations $q_{i,j} = f_i w - \frac{\mathrm{lc}(f_i)}{\mathrm{lc}(g_j)} u g_j$.
4. $F_{k+1} \coloneqq F_i \cup \{\mathrm{nf}_{\mathrm{RF}}(f) \mid f \in P_k \cup Q_k, \mathrm{nf}_{\mathrm{RF}}(f) \neq 0\}$, where $\mathrm{nf}_{\mathrm{RF}}(f)$ denotes the result of a right FG-reduction of f with F_k.
5. If $F_{k+1} \neq F_k$ increment k by one and go to step 2.
6. Return $F_\infty \coloneqq \bigcup F_k$.

By using Proposition 3.34, the reader will have no problem to proof the following.

Proposition 3.35 ([Nor01b, Proposition 9])**.** *F_∞ is a right FG-basis of the right ideal in $K\langle X \rangle / I$ generated by F.*

Remark. As already observed by Nordbeck in [Nor01b], we want to point out that we can also compute right FG-bases by using the regular two-sided Gröbner basis algorithm. For that we introduce a new "tag" variable and multiply it from the left to all one-sided generators. In the context of string rewriting systems, this trick was first introduced by Sims in [Sim94] (Section 2.8). A summary can be found on page 10 of [Rei98].

Chapter 4

Letterplace

In most modern computer algebra systems algorithms and data structures are highly optimized for commutative structures only. They are backed by research from the last 50 years and are ever since improved. Usually these systems provide little to no support for computations in noncommutative structures such as the free associative algebra. Rewriting the core algorithms and designing new noncommutative data structures in a performant manner is a nontrivial task.

In [LSL09] and [LSL13] Viktor Levandovskyy and Roberto La Scala introduced the *Letterplace ring*, which provided a new method for computing noncommutative Gröbner bases. They have embedded the free associative algebra in a suitable commutative polynomial ring, thus allowing us to reuse commutative data structures. The commutative core algorithms, such as the Buchberger algorithm or the reduction procedure, can be partially reused when slight modifications are made.

Before we begin, note that the way we will present the Letterplace ring is slightly different than originally in [LSL09] and [LSL13]. Our goal is to use the idea of the Letterplace ring as a tool to reuse commutative data structures for noncommutative computations in a computer algebra system.

4.1 The Letterplace Ring

The idea is simple: Enumerate the variables of a word in the order that they are occurring. After that, the variables can be commuted without losing the information about their order. In the Letterplace ring the enumeration is achieved by assigning a fixed *place* to each variable of a word. Therefore there are several copies of the original variables for different places. To keep the number of variables finite, an upper bound for the highest place has to be specified in advance. Hence, only words shorter than the upper bound can be represented in the resulting Letterplace ring. Consider the K-vector subspace of the free associative algebra $K\langle x_1, \ldots, x_n\rangle$ including only polynomials up to degree $d \in \mathbb{N}$. The corresponding Letterplace ring with *degree bound* d is the commutative polynomial ring

$$K[x_1(1), \ldots, x_n(1), x_1(2), \ldots, x_n(2), \ldots, x_1(d), \ldots, x_n(d)].$$

For the remaining of this chapter let d denote an arbitrary but fixed degree bound. The variable $x_j(i)$ stands for the original variable x_j at place i. The

word $x_1x_2x_1$, for example, corresponds to the monomial $x_1(1)\,x_2(2)\,x_1(3)$ in the Letterplace ring. To be more precise, for a word $w = x_{i_1}\cdots x_{i_k} \in \langle x_1,\ldots,x_n\rangle$ with $|w| \leq d$ we define the corresponding monomial $\mathrm{lp}(w) \coloneqq x_{i_1}(1)\cdots x_{i_k}(k)$ in the Letterplace ring and for the empty word ε we set $\mathrm{lp}(\varepsilon) \coloneqq 1$. We extend lp by K-linearity to all $f \in K\langle x_1,\ldots,x_n\rangle$ with $\deg(f) \leq d$. For a set of polynomials $F \subset K\langle x_1,\ldots,x_n\rangle$ we also write $\mathrm{lp}(F) \coloneqq \{\mathrm{lp}(f) \mid f \in F\}$.

It is easy to see that lp is injective. However, lp is not a bijection, in other words, not every monomial in the Letterplace ring corresponds to a word in the free associative algebra. The monomials which do correspond to a word in the free associative algebra are the monomial 1 and the ones that have exactly one variable for each place from 1 to the place of the variable with the highest place in the monomial. We call those monomials *Letterplace monomials* and we call a polynomial a *Letterplace polynomial* if it is a K-linear combination of Letterplace monomials. In other words, the image of lp is precisely the set of Letterplace polynomials and is denoted by $\mathrm{lp}(K\langle x_1,\ldots,x_n\rangle)$. Therefore, the left inverse map $\mathrm{lp}^{-1}\colon \mathrm{lp}(K\langle x_1,\ldots,x_n\rangle) \to K\langle x_1,\ldots,x_n\rangle$ of lp such that $\mathrm{lp}^{-1}(\mathrm{lp}(f)) = f$ for all $f \in K\langle x_1,\ldots,x_n\rangle$ with $\deg(f) \leq d$ is well defined.

For a Letterplace monomial $m = x_{i_1}(1)\cdots x_{i_k}(k)$ and $s \in \{0,\ldots,d-k\}$ we define

$$\mathrm{shift}(m,s) \coloneqq x_{i_1}(1+s)\cdots x_{i_k}(k+s).$$

We also say a monomial m' is *a shift of* a Letterplace monomial m, or simply m' is *shifted*, if $m' = \mathrm{shift}(m,s)$ for some $s \neq 0$. Furthermore, we call s the *shift of* m'. For convenience, we also define $\mathrm{shift}(c\cdot m,s) \coloneqq c\cdot\mathrm{shift}(m,s)$ for a polynomial $c\cdot m$ with $c \in K$ and m and s as before.

The length of a Letterplace monomial m, denoted by $|m|$, is the length of the corresponding word in the free associative algebra.

While we can use the normal addition for Letterplace monomials, the commutative multiplication of Letterplace monomials does not result in a Letterplace monomial. To be compatible with the multiplication of the free associative algebra we define the *Letterplace multiplication* $\times_{\mathrm{LP}}$ for two Letterplace monomials m and m' with $|m| + |m'| \leq d$ as

$$m \times_{\mathrm{LP}} m' \coloneqq m \cdot \mathrm{shift}(m', |m|).$$

It is easy to see that this gives us

$$\mathrm{lp}(w) \times_{\mathrm{LP}} \mathrm{lp}(w') = \mathrm{lp}(ww'),$$

for all $w, w' \in \langle x_1,\ldots,x_n\rangle$ with $|w| + |w'| \leq d$. Given a multiplication for monomials, the multiplication for polynomials follows naturally and we also get

$$\mathrm{lp}(f) \times_{\mathrm{LP}} \mathrm{lp}(f') = \mathrm{lp}(f\cdot f'),$$

for all $f, f' \in K\langle x_1,\ldots,x_n\rangle$ with $\deg(f) + \deg(f') \leq d$.

Equally, the divisibility of Letterplace monomials does not make sense yet. To obtain the same divisibility as in the free associative algebra we define the *Letterplace divisibility* $|_{\mathrm{LP}}$ for two Letterplace monomials m and m' as

$$m \,|_{\mathrm{LP}}\, m' \iff \exists s \in \{0,\ldots,d-|m|\}\colon\ \mathrm{shift}(m,s) \mid m'.$$

Again, it is easy to see that this gives us

$$\mathrm{lp}(w) \,|_{\mathrm{LP}}\, \mathrm{lp}(w') \iff w \mid w',$$

for all $w, w' \in \langle x_1, \ldots, x_n \rangle$ with $|w| \leq d$ and $|w'| \leq d$.

Together with the Letterplace multiplication and divisibility we can now embed all computations from the free associative algebra in the Letterplace ring as long as no polynomial with a degree larger than the degree bound d occurs.

There still remains an important detail which is not obvious from the beginning on. As we already know, the Gröbner basis of an ideal depends on the monomial ordering. Therefore, we need an ordering on the Letterplace ring with

$$\mathrm{lp}(w) \prec \mathrm{lp}(w') \iff w \prec w' \tag{4.1}$$

for $w, w' \in \langle x_1, \ldots, x_n \rangle$. For some orderings on the free associative algebra it is easy to construct an ordering on the Letterplace ring that satisfies (4.1) out of an ordering that is already available. Consider for example the degree left lexicographic ordering with $x_1 \succ \cdots \succ x_n$ on the free associative algebra. It is not hard to see that the equivalent ordering on the Letterplace ring is the degree left lexicographic ordering with

$$x_1(1) \succ \cdots \succ x_n(1) \succ \cdots \succ x_1(d) \succ \cdots \succ x_n(d).$$

4.2 Gröbner Bases in Singular via Letterplace

The Gröbner basis algorithm in SINGULAR via Letterplace is implemented as in Algorithm 5. Given a set of Letterplace polynomials $F \subset \mathrm{lp}(K\langle X \rangle)$, the algorithm returns a set of Letterplace polynomials $S \subset \mathrm{lp}(K\langle X \rangle)$ such that $\mathrm{lp}^{-1}(S)$ is a reduced Gröbner basis of $\langle \mathrm{lp}^{-1}(F) \rangle$.

Algorithm 5 Gröbner basis algorithm

```
procedure GröbnerBasis(F)
    S ← ∅
    T ← ∅
    L ← {(0, 0 , f) | f ∈ F \ {0}}
    while L ≠ ∅ do
        choose (a, b , p) ∈ L
        L ← L \ {(a, b , p)}
        if p = 0 then
            p ← SPolynomial(a, b)
        p ← Reduce(p, T)
        if p ≠ 0 then
            p ← (1/ lc(p)) · p
            for s ∈ {0, . . . , d − deg(p)} do
                T ← T ∪ {LmShift(p, s)}
            for f ∈ S do
                for s ∈ {0, . . . , d − deg(p)} do
                    q ← LmShift(p, s)
                    L ← InsertPair(f, q , L)
                for s ∈ {1, . . . , d − deg(f)} do
                    q ← LmShift(f, s)
                    L ← InsertPair(p, q , L)
                if lm(p) |LP lm(f) then
                    S ← S \ {f}
            S ← S ∪ {p}
    S ← CompleteReduce(S, T)
    return S
```

We want to stress, that every operation is performed in the commutative polynomial ring, that is the underlying structure of the Letterplace ring. We explicitly use $\times_{\text{LP}}$ and $|_{\text{LP}}$ to simulate noncommutative multiplication and divisibility respectively, otherwise the commutative multiplication and divisibility are meant.

To better understand the algorithm, we will explain some of the notation before we explain the procedures used in the algorithm. There are three sets that we work with. First, the set S, this is where we build the "standard basis" or in our case Gröbner basis. When a new element of the Gröbner basis is found, we look for critical pairs with the elements of S. From time to time we remove superfluous elements from S to keep the number of new critical pairs to a minimum. This does not happen with the reductor set T, which is a superset of S, where we keep all generators that we have encountered during the computation. Therefore, all reductions are performed with respect to T, giving us a broader selection of reductors. And finally, there is the "lazy set"[1] L containing the critical pairs that have to be processed together with their *S-polynomials*. An S-polynomial is simply the commutative form of overlap relations. While in the noncommutative case a critical pair can have several

[1] "lazy" because the S-polynomial is computed on demand

overlap relations, in the commutative case a critical pair has exactly one "overlap relation" and it is called S-polynomial.

Let us look at the procedure that computes the S-polynomial for the critical pair f, f'. We assume that f is a Letterplace polynomial, but $\mathrm{lm}(f')$ can be shifted. A critical pair in this context corresponds to exactly one overlap of the corresponding pair in the free associative algebra which is uniquely determined by the shift of $\mathrm{lm}(f')$. Therefore, we either have $\mathrm{lm}(f) \times_{\mathrm{LP}} m_2 = m_1 \cdot \mathrm{lm}(f')$ or $\mathrm{lm}(f) = m_1 \cdot \mathrm{lm}(f') \cdot m_1'$ for some uniquely determined Letterplace monomials m_1, m_2 and a monomial m_1' which is a shift of some Letterplace monomial (m_1, m_2, m_1' are also allowed to be $1 \in K$). For a monomial w of the form

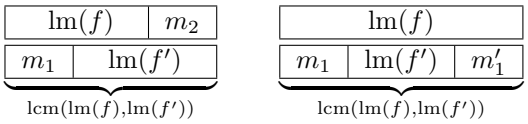


Figure 4.1: Visualization of m_1, m_1' and m_2

$w = w_1 \cdot \mathrm{shift}(w_2, s)$ with $s > |w_1|$ and Letterplace monomials w_1, w_2 we define

$$\mathrm{split}(w) \coloneqq (w_1, w_2).$$

If w is a Letterplace monomial, we define $\mathrm{split}(w) \coloneqq (w, 1)$. For a polynomial g we define

$$\mathrm{tail}(g) \coloneqq g - \mathrm{lt}(g).$$

Saving us a bit of work, we want to assume that $\mathrm{tail}(f')$ is a Letterplace polynomial while $\mathrm{lm}(f')$ can still be shifted. The problem is that for a Letterplace polynomial $g = \mathrm{lt}(g) + \mathrm{tail}(g)$ and some s we can have $\mathrm{shift}(\mathrm{lm}(g), s) \neq \mathrm{lm}(\mathrm{shift}(\mathrm{lt}(g), s) + \mathrm{tail}(g))$, therefore until the end of this chapter we redefine

$$\mathrm{lm}(\mathrm{shift}(\mathrm{lt}(g), s) + \mathrm{tail}(g)) \coloneqq \mathrm{shift}(\mathrm{lm}(g), s).$$

The ordering stays the same, what changes is that the leading monomial does not have to be the greatest monomial with respect to the ordering anymore. This is obviously only an implementation detail and less of a theoretical approach.

S-polynomial creation procedure

procedure SPolynomial(f, f')
  $m \leftarrow \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(f'))$ ▷ (commutative) least common multiple
  $m_1 \leftarrow m$ divided by $\mathrm{lm}(f')$
  $m_2 \leftarrow m$ divided by $\mathrm{lm}(f)$
  $(m_1, m_1') \leftarrow \mathrm{split}(m_1)$
  return $(\mathrm{tail}(f) \times_{\mathrm{LP}} m_2) - \left(\frac{\mathrm{lc}(f)}{\mathrm{lc}(f')} \cdot m_1 \times_{\mathrm{LP}} \mathrm{tail}(f') \times_{\mathrm{LP}} m_1'\right)$

Remark. Remember that $\mathrm{tail}(f)$ and $\mathrm{tail}(f')$ are Letterplace polynomials, therefore the procedure returns a Letterplace polynomial. Also, remember that the coefficient is chosen such that $\mathrm{lm}(f)$ and $\mathrm{lm}(f')$ cancel in the S-polynomial.

The pair insertion procedure checks whether f, f' is a critical pair and if this is the case, adds it to the set L. Because the critical pairs will be the input

for the S-polynomial procedure, we assume that f and $\mathrm{tail}(f')$ are Letterplace polynomials and only $\mathrm{lm}(f')$ can be shifted. As said before, each critical pair that is inserted corresponds to exactly one overlap which is uniquely determined by the shift of $\mathrm{lm}(f')$.

Pair insertion procedure

procedure InsertPair(f, f', L)
  $m \leftarrow \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(f'))$
  if $\mathrm{lm}(f) \cdot \mathrm{lm}(f') \neq m$ **and** m is a Letterplace monomial **then**
    return $L \cup \{(f, f', 0)\}$
  else
    return L

Example 4.1. Consider the polynomials $f_1 = x_1(1)x_1(2)$, $f_2 = x_1(1)x_2(2)$ and $f_3 = x_1(2)x_2(3)$, then f_1, f_2 and f_2, f_3 are no critical pairs, but f_1, f_3 is a critical pair.

The reduction procedure is quite similar to the S-polynomial procedure. We assume that p is a Letterplace polynomial. Instead of checking the divisibility with $|_{\mathrm{LP}}$, we use the commutative divisibility and assume that for every Letterplace polynomial $f \in T$ we also have that $\mathrm{shift}(\mathrm{lm}(f), s) + \mathrm{tail}(f)$ is in T for $s \in \{0, \ldots, d - \deg(f)\}$ and there are no other non Letterplace polynomials in T. Therefore, if there is a Letterplace polynomial $f \in T$ with $\mathrm{lm}(f) \,|_{\mathrm{LP}}\, \mathrm{lm}(p)$, then there is $f' \in T$ with $\mathrm{lm}(f') \mid \mathrm{lm}(p)$ and $\mathrm{tail}(f') = \mathrm{tail}(f)$.

Reduction procedure

procedure Reduce(p, T)
  while exists $f \in T$ with $\mathrm{lm}(f) \mid \mathrm{lm}(p)$ **do**
    $m \leftarrow \mathrm{lm}(p)$ divided by $\mathrm{lm}(f)$
    $(m_1, m_2) \leftarrow \mathrm{split}(m)$
    $p \leftarrow \mathrm{tail}(p) - \left(\frac{\mathrm{lc}(p)}{\mathrm{lc}(f)} \cdot m_1 \times_{\mathrm{LP}} \mathrm{tail}(f) \times_{\mathrm{LP}} m_2\right)$
  $p \leftarrow$ ReduceTail(p, T)
  return p

After reducing the leading monomial, the reduction procedure calls the almost identical tail reduction procedure for a complete reduction.

Tail reduction procedure

procedure ReduceTail(p, T)
  while exists $f \in T$ and $m \in \mathrm{supp}(p)$ with $\mathrm{lm}(f) \mid m$ **do**
    $c \leftarrow$ the coefficient of m in p
    $p \leftarrow p - c \cdot m$
    $m \leftarrow m$ divided by $\mathrm{lm}(f)$
    $(m_1, m_2) \leftarrow \mathrm{split}(m)$
    $p \leftarrow p - \left(\frac{c}{\mathrm{lc}(f)} \cdot m_1 \times_{\mathrm{LP}} \mathrm{tail}(f) \times_{\mathrm{LP}} m_2\right)$
  return p

The reduction procedure was split into two parts, because the tail reduction is used again in the complete reduction procedure at the end of the algorithm. The procedure ensures that $\mathrm{lp}^{-1}(S)$ is reduced as in Definition 3.21. We assume that $\mathrm{lp}^{-1}(S)$ is a Gröbner basis, the polynomials in S are monic and no leading monomial of a polynomial in S divides (using Letterplace division) the leading monomial of another polynomial in S, thus $\mathrm{lt}(\mathrm{lp}^{-1}(S))$ is already reduced. Therefore, for $\mathrm{lp}^{-1}(S)$ to be reduced, it is sufficient to reduce only the tail of the polynomials in S.

Complete reduction procedure

```
procedure CompleteReduce(S, T)
    S' ← ∅
    for f ∈ S do
        S' ← S' ∪ {ReduceTail(f, T)}
    return S'
```

The polynomials with the shifted leading monomials that we have seen in T and L come from the leading monomial shift procedure. It is self-explanatory and has been moved into its own procedure for readability.

Leading monomial shift procedure

```
procedure LmShift(p, s)
    return shift(lt(p), s) + tail(p)
```

Remark. We have left out some performance improvements that Singular does in Algorithm 5. For example, the leading monomials of the overlap relations in L are computed immediately and then the elements in L are sorted with respect to certain selection strategies based on the leading monomials. The selection strategy has an important effect on the number of overlap relations that need to be processed during the computation and therefore an effect on the efficiency. With the *normal strategy* for example, the elements are sorted in ascending order by their leading monomials. If an overlap relation is not completely reduced after a certain number of steps, the reduction is postponed and the intermediate result is reinserted into L for later processing at which point there might be new reductors that make the reduction faster. With certain criteria, it is possible to identify some critical pairs that will reduce to zero without actually reducing them. More about criteria and selection strategies can be found, for example, in [Alu06] (Section 3.4).

Remark. In practice, options to for example skip the tail reduction or the normalization are are also available. A complete list of options can be found in the Singular Manual at `https://www.singular.uni-kl.de/Manual/4-1-1/sing_315.htm#SEC355`.

4.3 Right Factor-Gröbner Bases in Singular via Letterplace

As a part of this thesis, we have implemented the right FG-basis algorithm in Singular via Letterplace as in Algorithm 6. Let $Q \subset \mathrm{lp}(K\langle X\rangle)$ be a set of Letterplace polynomials and $\mathrm{lp}^{-1}(Q)$ a Gröbner basis for the ideal $I \subset K\langle X\rangle$. Given Q and a set of Letterplace polynomials $F \subset \mathrm{lp}(K\langle X\rangle)$, the algorithm returns a set of Letterplace polynomials $S \subset \mathrm{lp}(K\langle X\rangle)$ such that $\mathrm{lp}^{-1}(S)$ is a reduced right FG-basis of the right ideal generated by $\mathrm{lp}^{-1}(F)$ in $K\langle X\rangle/I$.

Algorithm 6 right FG-basis algorithm

```
procedure RightFGBasis(F, Q)
    S ← Q
    T ← {LmShift(f, s) | ∀f ∈ Q, ∀s ∈ {0, ..., d − deg(f)}}
    L ← {(0, 0 , f) | f ∈ F \ {0}}
    while L ≠ ∅ do
        choose (a, b , p) ∈ L
        L ← L \ {(a, b , p)}
        if p = 0 then
            p ← SPolynomial(a, b)
        p ← Reduce(p, T)
        if p ≠ 0 then
            p ← (1/ lc(p)) · p
            T ← T ∪ {p}
            for f ∈ S do
                L ← InsertPair(f, p , L)
                if f ∈ Q then
                    for s ∈ {1, ..., d − deg(f)} do
                        q ← LmShift(f, s)
                        L ← InsertPair(p, q , L)
                if lm(p) | lm(f) and f ∉ Q then
                    S ← S \ {f}
            S ← S ∪ {p}
    S ← S \ Q
    S ← CompleteReduce(S, T)
    return S
```

The meaning of the sets and the helper procedures stay the same as in Section 4.2. Solely the assumption for the input of the reduction procedure is slightly different. Earlier we have assumed that for every Letterplace polynomial $f \in T$ we also have that $\mathrm{shift}(\mathrm{lm}(f), s)+\mathrm{tail}(f)$ is in T for $s \in \{0, \ldots, d-\deg(f)\}$. Now we assume that this is only the case for $f \in Q$ and there are no other non Letterplace polynomials in T. This gives us the desired effect that during the reduction elements from Q can be multiplied from both sides while elements not from Q can only be multiplied from the right-hand side. The new assumption already sums up the changes compared to the regular Gröbner basis algorithm. The only monomials that get shifted are the leading monomials of elements in Q, thus giving us the correct reduction and pair construction. Considering the

remark at the end of Section 3.6, this does not come as a surprise.

However, the implementation as in Algorithm 6 is much more efficient. To underline this, we have compared the two approaches in Example A.1.

Chapter 5

Dimension Computations

Let I be an ideal of $K\langle X\rangle$. We already know that $K\langle X\rangle$ is infinite-dimensional as a vector space. The question arises whether $K\langle X\rangle/I$ is finite-dimensional as a vector space and if so, whether we can compute its K-dimension. In this chapter we aim to answer these questions and further study the K-dimension $K\langle X\rangle/I$.

5.1 The Growth of Algebras and the Gelfand-Kirillov Dimension

Our main reference for this section is [KL99] where the growth of algebras and the Gelfand-Kirillov dimension are discussed in great detail.

Let A be a finitely generated K-algebra, that is there exists a finite *generating subset* $B \subset A$ in the sense that every element in A can be written as a K-linear combination of products formed with the elements of B. In this case there exists a finite-dimensional *generating subspace* $V \subset A$ (e.g., the vector space generated by B over K) in the following sense: If $V^0 = K$ and for $n \geq 1$ the subspace generated by all products of n elements of V is denoted by V^n, then

$$A = \bigcup_{n=0}^{\infty} A_n, \quad \text{where } A_n \coloneqq K + V + V^2 + \cdots + V^n.$$

Example 5.1. Consider $A = K\langle X\rangle$ with $X = \{x, y\}$. X is a generating subset of A and since X is finite, A is finitely generated. The subspace $V \subset A$ generated by X is a generating subspace of A. In this case the subspace V^n is generated by all words of length n in $\langle X\rangle$ and the subspace A_n consists of all polynomials in A up to degree n. The subspace V^2 is generated by $\{x^2, xy, yx, y^2\}$.

Example 5.2. Consider $A = K\langle X\rangle/I$ with $I = \langle y^2, yx^2\rangle \subset K\langle X\rangle$ and $X = \{x, y\}$. $B = \{x + I \mid x \in X\}$ is a finite generating subset of A and thus A is finitely generated. The subspace $V \subset A$ generated by B is a generating subspace of A. In this case the subspace V^n is generated by $\{w+I \in A \mid w \in \langle X\rangle, |w| = n\}$ and we have $A_n = \{f + I \in A \mid \deg(f) \leq n\}$. The subspace V^2 is generated by $\{x^2 + I, xy + I, yx + I, y^2 + I\}$. Since $y^2 \in I$, we have $y^2 + I = 0 + I$ and thus $y^2 + I$ is not part of the K-basis $\{x^2 + I, xy + I, yx + I\}$ of V^2.

Clearly, if A is finite-dimensional as a vector space, then we have $A = A_n$ for some n and the *dimension function* $d_V(n) \coloneqq \dim_K(A_n)$ has a finite maximum. Otherwise, d_V is a monotonously increasing function.

Definition 5.3. Let Φ denote the set of monotonously increasing functions $f\colon \mathbb{N} \to \mathbb{R}^+$. For $f, g \in \Phi$ we define the relation

$$f \preceq g \iff \text{there exist } c, m \in \mathbb{N} \text{ such that } f(n) \leq cg(mn) \text{ for all } n \in \mathbb{N},$$

and the equivalence

$$f \sim g \iff f \preceq g \text{ and } g \preceq f.$$

For $f \in \Phi$ we call the equivalence class $\mathcal{G}(f) \in \Phi/\!\sim$ the *growth* of f. The ordering on the set $\Phi/\!\sim$ induced by $\preceq$ is denoted by $\leq$.

A polynomial function of degree d has growth $\mathcal{G}(n^d)$. If $\mathcal{G}(f) = \mathcal{G}(n^d)$ for some d, we say f has polynomial growth of degree d. The growth $\mathcal{G}(2^n)$, is called exponential.

Lemma 5.4 ([KL99])**.** *Let A be a finitely generated K-algebra with finite-dimensional generating subspaces V and W. If $d_V(n)$ and $d_W(n)$ denote the dimensions of $\sum_{i=0}^n V^i$ and $\sum_{i=0}^n W^i$ respectively, then $\mathcal{G}(d_V) = \mathcal{G}(d_W)$.*

Proof. Since

$$A = \bigcup_{n=0}^{\infty} (V^0 + \cdots + V^n) = \bigcup_{n=0}^{\infty} (W^0 + \cdots + W^n),$$

there exist $s, t \in \mathbb{N}$ such that

$$W \subseteq \sum_{i=0}^{s} V^i \quad \text{and} \quad V \subseteq \sum_{i=0}^{t} W^i.$$

Thus $d_W(n) \leq d_V(sn)$ and $d_V(n) \leq d_W(tn)$. □

With the last result in mind, it becomes obvious that the growth of d_V is determined by the algebra itself and independent of the choice of V.

Definition 5.5. Let A be a finitely generated K-algebra and let V be a finite-dimensional generating subspace of A. We call $\mathcal{G}(A) \coloneqq \mathcal{G}(d_V)$ the *growth* of A.

We note that the growth of A does not depend on a monomial ordering.

Lemma 5.6 ([BK76])**.** *Let A be a finitely generated K-algebra, then $\mathcal{G}(A) \leq \mathcal{G}(2^n)$.*

Proof. Let V be a finite-dimensional generating subspace of A with $1 \in V$. Then

$$d_V(n) = \dim_K \left(\sum_{i=0}^{n} V^i \right) = \dim_K (V^n) \leq \dim_K (V)^n,$$

and thus $\mathcal{G}(A) = \mathcal{G}(d_V) \leq \mathcal{G}(2^n)$. □

Definition 5.7. Let A be a finitely generated K-algebra with finite-dimensional generating subspace V. The *Gelfand-Kirillov dimension*, or simply *GK-dimension*, of A is defined as

$$\mathrm{GKdim}(A) \coloneqq \varlimsup_{n\to\infty} \log_n d_V(n) = \inf\{d \in \mathbb{R} \mid \mathcal{G}(d_V) \leq \mathcal{G}(n^d)\}.$$

Clearly, for a finitely generated K-algebra A we have $\mathrm{GKdim}(A) = 0$ if and only if A is finite-dimensional as a vector space. Moreover, if $\mathrm{GKdim}(A) = \infty$, then A does not have polynomial growth.

Example 5.8. Consider $A = K\langle X\rangle$ with $X = \{x, y\}$. The subspace V generated by X is a generating subspace of A. Clearly $V^i \cap V^j = \{0\}$ holds for $i \neq j$, which means we can use the direct sum $\oplus$ of vector spaces. We have

$$\begin{aligned} d_V(n) &= \dim_K(K + V + V^2 + \cdots + V^n) \\ &= \dim_K(K \oplus V \oplus V^2 \oplus \cdots \oplus V^n) \\ &= 1 + 2 + 2^2 + \cdots + 2^n \\ &= 2^{n+1} - 1. \end{aligned}$$

Therefore the growth of A is exponential and $\mathrm{GKdim}(A) = \infty$.

From Example 5.8 it is clear that for $|X| > 1$ the growth of $K\langle X\rangle$ is exponential and therefore $\mathrm{GKdim}(K\langle X\rangle) = \infty$. By the same argument, for $|X| = 1$ the growth of $K\langle X\rangle$ is linear, that is $\mathcal{G}(n)$ and we have $\mathrm{GKdim}(K\langle X\rangle) = 1$. We are now interested in the GK-dimension of the factor algebra $K\langle X\rangle/I$ for an ideal I of $K\langle X\rangle$. Therefore we first state a useful Lemma.

Lemma 5.9. *Let I be an ideal of $K\langle X\rangle$, let V be the generating subspace of $K\langle X\rangle/I$ generated by $\{x + I \mid x \in X\}$ and let W be the generating subspace of $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ generated by $\{x + \langle \mathrm{lm}(I)\rangle \mid x \in X\}$. If the monomial ordering on $\langle X\rangle$ is length-compatible, then the dimension functions d_V and d_W are equal.*

Proof. We have that V^n is generated by $\{w + I \mid w \in \langle X\rangle, |w| = n\}$ and W^n is generated by $\{w + \langle \mathrm{lm}(I)\rangle \mid w \in \langle X\rangle, |w| = n\}$ for all n. It follows that $\sum_{i=0}^n V^i$ is generated by $S_V^{(n)} = \{w + I \mid w \in \langle X\rangle, |w| \leq n\}$ and $\sum_{i=0}^n W^i$ is generated by $S_W^{(n)} = \{w + \langle \mathrm{lm}(I)\rangle \mid w \in \langle X\rangle, |w| \leq n\}$. We claim that $B_V^{(n)} = \{w + I \mid w \in \langle X\rangle \text{ is normal modulo } I, |w| \leq n\}$ and $B_W^{(n)} = \{w + \langle \mathrm{lm}(I)\rangle \mid w \in \langle X\rangle \text{ is normal modulo } I, |w| \leq n\}$ are K-bases of $\sum_{i=0}^n V^i$ and $\sum_{i=0}^n W^i$ respectively. Clearly the elements in $B_V^{(n)}$ and $B_W^{(n)}$ are K-linear independent. It remains to show that $B_V^{(n)}$ and $B_W^{(n)}$ generate $\sum_{i=0}^n V^i$ and $\sum_{i=0}^n W^i$ respectively. Clearly $B_V^{(n)} \subset \sum_{i=0}^n V^i$ and $B_W^{(n)} \subset \sum_{i=0}^n W^i$. We further show that for every $w \in \langle X\rangle$ with $|w| \leq n$, the elements $w + I \in S_V^{(n)}$ and $w' + \langle \mathrm{lm}(I)\rangle \in S_W^{(n)}$ are K-linear combinations of elements in $B_V^{(n)}$ and $B_W^{(n)}$ respectively. Note that these are precisely the elements in $S_V^{(n)}$ and $S_W^{(n)}$. If w is normal modulo I, then $w + I \in B_V^{(n)}$ and $w + \langle \mathrm{lm}(I)\rangle \in B_W^{(n)}$. Now assume w is not normal modulo I. For the case that $\mathrm{nf}_I(w) = 0$, we have $w + I = 0 + I$ which is obviously a K-linear combination of elements in $B_V^{(n)}$. Otherwise, for every $w' \in \mathrm{supp}(\mathrm{nf}_I(w))$, we have that w' is normal modulo I and since by assumption the monomial ordering is length-compatible, $|w'| \leq |w| \leq n$. It follows

that $w + I = \mathrm{nf}_I(w) + I$ is a K-linear combination of elements in $B_V^{(n)}$. Clearly we have $w + \langle \mathrm{lm}(I)\rangle = 0 + \langle \mathrm{lm}(I)\rangle$ which is a K-linear combination of elements in $B_W^{(n)}$. We have now proven that $B_V^{(n)}$ and $B_W^{(n)}$ are K-bases for $\sum_{i=0}^n V^i$ and $\sum_{i=0}^n W^i$ respectively. From the definition it is clear that $|B_V^{(n)}| = |B_W^{(n)}|$ and thus we get

$$d_V(n) = \dim_K \left(\sum_{i=0}^{n} V^i \right) = |B_V^{(n)}| = |B_W^{(n)}| = \dim_K \left(\sum_{i=0}^{n} W^i \right) = d_W(n).$$

□

Now the following proposition follows immediately.

Proposition 5.10. *Let I be an ideal of $K\langle X\rangle$. If the monomial ordering on $\langle X\rangle$ is length-compatible, then $K\langle X\rangle/I$ and $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ have the same growth and thus the same GK-dimension.*

Remark. A length-compatible ordering on $\langle X\rangle$ is only a sufficient but not a necessary condition. Suppose there exists $c \in \mathbb{N}$ such that

$$\max\{|w'| : w' \in \mathrm{supp}(\mathrm{nf}_I(w))\} \leq c\,|w| \tag{5.1}$$

for all $w \in \langle X\rangle$. Then, using the generating subspaces V generated by $\{x + I \mid x \in X\}$ and W generated by $\{x + \langle \mathrm{lm}(I)\rangle \mid x \in X\}$ of $K\langle X\rangle/I$ and $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ respectively and reconsidering the proof of Lemma 5.9, it is easy to see that $d_V(n) \preceq d_W(cn)$ for all n. We will see in Lemma 5.9 that we always have $d_W \preceq d_V$. It follows that if (5.1) holds, then $K\langle X\rangle/I$ and $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ have the same growth and thus the same GK-dimension. Note that we were not able to verify whether (5.1) is a necessary condition.

From the proof of Lemma 5.9 also follows

Lemma 5.11. *Let M be a finite subset of $\langle X\rangle$ and choose $V = \{x + \langle M\rangle \mid x \in X\}$ as a generating subspace of $K\langle X\rangle/\langle M\rangle$. Then for all n, $d_V(n)$ is equal to the number of words of length not greater than n that are normal modulo $\langle M\rangle$.*

The following lemma is a new result. In particular, that the GK-dimension of $K\langle X\rangle/I$ can be greater than the GK-dimension of $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$. We will give an example for this in Example 5.23.

Lemma 5.12. *Let I be an ideal of $K\langle X\rangle$. For every monomial ordering on $\langle X\rangle$, the growth of $K\langle X\rangle/I$ is greater than or equal to the growth of $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ and thus the GK-dimension of $K\langle X\rangle/I$ is greater than or equal to the GK-dimension of $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$.*

Proof. Choose the generating subspaces V generated by $\{x + I \mid x \in X\}$ and W generated by $\{x + \langle \mathrm{lm}(I)\rangle \mid x \in X\}$ of $K\langle X\rangle/I$ and $K\langle X\rangle/\langle \mathrm{lm}(I)\rangle$ respectively. Then by Lemma 5.11, for all n, $d_W(n)$ is equal to the number of words of length not greater than n that are normal modulo $\langle \mathrm{lm}(I)\rangle$. The subset

$$\{w + I \mid w \in \langle X\rangle \text{ is normal modulo } \langle \mathrm{lm}(I)\rangle \text{ and } |w| \leq n\} \subset \sum_{i=0}^{n} V^i$$

contains $d_W(n)$ pairwise K-linear independent elements and thus for all n,

$$d_V(n) = \dim_K \left(\sum_{i=0}^{n} V^i \right) \geq d_W(n).$$

□

Example 5.13. Consider $X = \{x, y\}$ and the ideal $I = \langle xy - y \rangle$ of $K\langle X \rangle$. Assume a length-compatible monomial ordering on $\langle X \rangle$, for example the degree left lexicographic ordering with $x \succ y$. The subspace V generated by $\{x + \langle \operatorname{lm}(I) \rangle, y + \langle \operatorname{lm}(I) \rangle\}$ is a generating subspace of $K\langle X \rangle / \langle \operatorname{lm}(I) \rangle$. The set $N_n = \{y^i x^j \mid i + j = n\}$ contains precisely the words of length n that are normal modulo I. We have $|N_n| = n + 1$, and therefore by Lemma 5.11

$$\begin{aligned} d_V(n) &= |N_0| + |N_1| + |N_2| + \cdots + |N_n| \\ &= 1 + 2 + 3 + \cdots + (n+1) \\ &= \frac{(n+1)^2 + (n+1)}{2}. \end{aligned}$$

Hence, the growth of $K\langle X \rangle / \langle \operatorname{lm}(I) \rangle$ is $\mathcal{G}(n^2)$ and the GK-dimension of $K\langle X \rangle / \langle \operatorname{lm}(I) \rangle$ is 2. By Proposition 5.10, the growth of $K\langle X \rangle / I$ is also $\mathcal{G}(n^2)$ and thus the GK-dimension of $K\langle X \rangle / I$ is also 2.

Example 5.14. Consider $X = \{x, y\}$ and the ideal $I = \langle xy - y^3 \rangle$ of $K\langle X \rangle$. For every length-compatible monomial ordering on $\langle X \rangle$, we have $y^3 \succ xy$ and the reader can verify that no finite Gröbner basis of I exists for such an ordering. Now assume a monomial ordering on $\langle X \rangle$ such that $xy \succ y^3$. Then $\{xy - y^3\}$ is already a Gröbner basis of I. By Example 5.13 we already know that the GK-dimension of $K\langle X \rangle / \langle \operatorname{lm}(I) \rangle$ is 2. Since we have not assumed a length-compatible monomial ordering, for now we only know by Lemma 5.12 that the GK-dimension of $K\langle X \rangle / I$ is at least 2. For all $w \in \langle X \rangle$ the normal form of w modulo I is a word. It is easily seen that among all $w \in \langle X \rangle$ with $|w| = n$, the normal form of w modulo I becomes longest for $w = x^{n-1}y$ and in this case $\operatorname{nf}_I(w) = y^{2n-1}$. It follows that

$$\max \{|w'| : w' \in \operatorname{supp}(\operatorname{nf}_I(w))\} = |\operatorname{supp}(\operatorname{nf}_I(w))| \leq 2\,|w|$$

for all $w \in \langle X \rangle$ as in (5.1). By the remark after 5.10 we can now safely conclude that the GK-dimension of $K\langle X \rangle / I$ is also 2.

5.2 Computing the Gelfand-Kirillov dimension

In the previous section we have already shown that the GK-dimension of $K\langle X \rangle$ is either 1 or ∞ and in Example 5.13 and Example 5.14 we have computed the GK-dimension of two factor algebras of $K\langle X \rangle$. However, the examples were carefully chosen such that we could easily compute the GK-dimension. In general, computing the GK-dimension of $K\langle X \rangle / I$ for an ideal I of $K\langle X \rangle$ is not so trivial. In this section we work towards an algorithm to compute the GK-dimension of $K\langle X \rangle / I$ by using Gröbner bases and the *Ufnarovski graph*.

Definition 5.15. Let M be a non-empty reduced finite subset of $\langle X\rangle \setminus \{\varepsilon\}$ and let

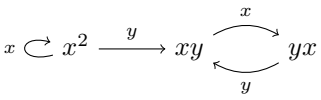
$$l = \max\{|w| : w \in M\} - 1.$$

The *Ufnarovski graph* of M has the set of vertices

$$V = \{v \in \langle X\rangle \mid v \text{ is normal modulo } \langle M\rangle,\ |v| = l\}.$$

For every two vertices $v, v' \in V$ there is a directed edge from v to v' if and only if there exist $x_i, x_j \in X$ such that $vx_i = x_j v'$ and such that vx_i is normal modulo $\langle M\rangle$. This edge will be labeled by x_i.

Example 5.16. Consider $M = \{y^2,\ yx^2\} \subset \langle x, y\rangle$. Then we have $l = 2$ and $V = \{x^2,\ xy,\ yx\}$. The Ufnarovski graph of M is presented by



Definition 5.17. Let $\Gamma = (V, E)$ be a directed graph.

1. A *route* of length $m \geq 1$ in Γ is a sequence of vertices $v_0, v_1, \ldots, v_m \in V$ such that $(v_i, v_{i+1}) \in E$ for all $i \in \{0, \ldots, m-1\}$.
2. A *cycle* in Γ is a route $v_0, v_1, \ldots, v_m$ such that $v_0 = v_m$ and $v_0, v_1, \ldots, v_{m-1}$ are pairwise distinct.

A cycle of length 1 is also called a *loop*. For convenience we consider a single vertex as a route of length 0.

The following lemma describes the essential property of the Ufnarovski graph (originally in [Ufn82]).

Lemma 5.18. *Let M be a non-empty reduced finite subset of $\langle X\rangle \setminus \{\varepsilon\}$, let Γ be the Ufnarovski graph of M and let $l = \max\{|w| : w \in M\} - 1$. There is a one-to-one correspondence between the routes of length $m \in \mathbb{N}_0$ in Γ and the words of length $m + l$ that are normal modulo $\langle M\rangle$.*

Proof. For every word $w = x_1 \cdots x_{m+l}$ of length $m + l$ with $x_1, \ldots, x_{m+l} \in X$ that is normal modulo $\langle M\rangle$, we uniquely associate the route

$$v_0, v_1, \ldots, v_m \quad \text{where } v_i = x_{i+1} \cdots x_{i+l}.$$

Conversely, for every route $v_0, v_1, \ldots, v_m$ of length m in Γ we have $v_i = x_{i+1} \cdots x_{i+l}$ for some $x_1, \ldots, x_{m+l} \in X$ and we uniquely associate the word $x_1 \cdots x_{m+l}$ of length $m + l$ that is normal modulo $\langle M\rangle$. □

The route x^2, xy, yx in the graph from Example 5.16, for example, corresponds to the word x^2yx.

Definition 5.19. Let Γ be a graph and let d_Γ be the function where $d_\Gamma(n)$ is the number of routes of length n in Γ. We call $\mathcal{G}(\Gamma) \coloneqq \mathcal{G}(d_\Gamma)$ the *growth* of Γ.

Theorem 5.20 ([Ufn82])**.** *Let Γ be a graph. The growth of Γ is either exponential or polynomial. More precisely,*

1. *The growth of* Γ *is exponential if and only if there are two distinct cycles with a common vertex in* Γ.

2. *Otherwise, the growth of* Γ *is polynomial of degree* d*, where* d *is the maximal number of distinct cycles occurring in a single route of* Γ.

□

Proposition 5.21 ([Ufn82])**.** *Let* M *be a non-empty reduced finite subset of* $\langle X\rangle \setminus \{\varepsilon\}$ *and let* Γ *be the Ufnarovski graph of* M*. The growth of* Γ *is equal to the growth of* $K\langle X\rangle/\langle M\rangle$.

Proof. Choose $V = \{x + \langle M\rangle \mid x \in X\}$ as a generating subspace of $K\langle X\rangle/\langle M\rangle$, let $l = \max\{|w| : w \in M\} - 1$ and let $c = d_V(l)$. By Lemma 5.11 and Lemma 5.18 we have

$$d_V(n) = c + d_\Gamma(n - l).$$

It is now easily seen that $\mathcal{G}(d_V) = \mathcal{G}(\Gamma)$. □

Theorem 5.22. *Let* $G \subset K\langle X\rangle \setminus \{1\}$ *be a non-empty reduced finite Gröbner basis, let* $I = \langle G\rangle$ *and let* Γ *be the Ufnarovski graph of* $\operatorname{lm}(G)$*. The growth of* $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ *and the growth of* $K\langle X\rangle/I$ *is either exponential or polynomial. More precisely,*

1. *The growth of* $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ *is exponential if and only if there are two distinct cycles with a common vertex in* Γ*. If the growth of* $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ *is exponential, then the growth of* $K\langle X\rangle/I$ *is exponential and we have*

$$\operatorname{GKdim}(K\langle X\rangle/I) = \operatorname{GKdim}(K\langle X\rangle/\langle \operatorname{lm}(I)\rangle) = \infty.$$

2. *If the growth of* $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ *is not exponential, then it is polynomial of degree* d*, where* d *is the maximal number of distinct cycles occurring in a single route of* Γ*. If the monomial ordering on* $\langle X\rangle$ *is length-compatible, then*

$$\operatorname{GKdim}(K\langle X\rangle/I) = \operatorname{GKdim}(K\langle X\rangle/\langle \operatorname{lm}(I)\rangle) = d.$$

   Otherwise,

$$\operatorname{GKdim}(K\langle X\rangle/I) \geq \operatorname{GKdim}(K\langle X\rangle/\langle \operatorname{lm}(I)\rangle) = d.$$

   If $d = 0$*, then* $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ *and* $K\langle X\rangle/I$ *are finite-dimensional vector spaces of the same dimension. In this case we have*

$$\operatorname{GKdim}(K\langle X\rangle/I) = \operatorname{GKdim}(K\langle X\rangle/\langle \operatorname{lm}(I)\rangle) = 0.$$

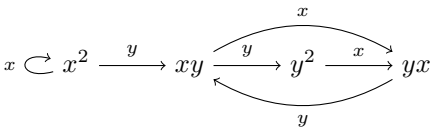
Proof. By Proposition 3.2 we have $\langle \operatorname{lm}(G)\rangle = \langle \operatorname{lm}(I)\rangle$ and thus by Theorem 5.20 and Proposition 5.21 all statements about $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ hold. By Proposition 3.20 if $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ is a finite-dimensional vector space, then $K\langle X\rangle/I$ is a finite-dimensional vector space of the same dimension. If the monomial ordering on $\langle X\rangle$ is length-compatible, then by Proposition 5.10 $K\langle X\rangle/I$ and $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ have the same GK-dimension and we are done. Now assume that the monomial ordering on $\langle X\rangle$ is not length-compatible. By Lemma 5.12 the GK-dimension of $K\langle X\rangle/I$ is greater than or equal to the GK-dimension of $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$. By Lemma 5.6 the growth of $K\langle X\rangle/I$ is not greater than exponential. □

Remark. A similar theorem has been stated in [Xiu12] and [Li11]. However, in [Xiu12] it is only defined for length-compatible monomial orderings and in [Li11] there is no distinction between the case of a length-compatible monomial ordering and the case of a monomial ordering that is not length-compatible. In Example 5.23 it will become clear that this distinction must be made.

As we know from Proposition 3.20, for every ideal I of $K\langle X\rangle$, $K\langle X\rangle/I$ and $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$ are isomorphic as vector spaces. It seems counter intuitive at first that the growth of $K\langle X\rangle/I$ might be greater than the growth of $K\langle X\rangle/\langle \operatorname{lm}(I)\rangle$, but the following example shows that this can indeed be the case.

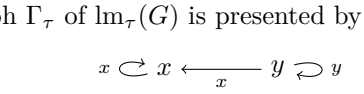
Example 5.23. Consider $X = \{x, y\}$ and the ideal $I = \{yx^2 - xy\}$. For an arbitrary monomial ordering on $\langle X\rangle$ we either have $yx^2 \succ xy$ or $xy \succ yx^2$ and in both cases $yx^2 - xy$ does not give rise to any overlap relations. Therefore $G = \{yx^2 - xy\}$ is a reduced Gröbner basis with respect to an arbitrary monomial ordering. During this example, $\operatorname{lm}_\sigma(F)$ denotes the set of leading monomials of a subset $F \subset K\langle X\rangle$ with respect to a monomial ordering σ.

Let σ be an arbitrary length-compatible monomial ordering. G is a Gröbner basis with respect to σ and we have $\operatorname{lm}_\sigma(G) = \{yx^2\}$. The Ufnarovski graph Γ_σ of $\operatorname{lm}_\sigma(G)$ is presented by



Clearly, xy, y^2, yx, xy and xy, yx, xy are two distinct cycles in Γ_σ with a common vertex and thus by Theorem 5.22 $K\langle X\rangle/\langle \operatorname{lm}_\sigma(I)\rangle$ and $K\langle X\rangle/I$ both have infinite GK-dimension.

Now consider some monomial ordering τ such that xy is greater than yx^2. One example of such a monomial ordering is the wreath product [Sim94]. G is also a Gröbner basis with respect to τ but this time we have $\operatorname{lm}_\tau(G) = \{xy\}$. The Ufnarovski graph Γ_τ of $\operatorname{lm}_\tau(G)$ is presented by



Clearly x, x and y, y are the only cycles in Γ_τ and they do not have a common vertex. Since 2 is the maximal number of distinct cycles occurring in a single route of Γ_τ, by Theorem 5.22 the GK-dimension of $K\langle X\rangle/\langle \operatorname{lm}_\tau(I)\rangle$ is equal to 2. Note that this is also confirmed by the result of Example 5.13.

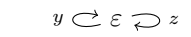
Let $A = K\langle X\rangle/\langle I\rangle$, $A_{\operatorname{lm}\tau} = K\langle X\rangle/\langle \operatorname{lm}_\tau(I)\rangle$ and $A_{\operatorname{lm}\sigma} = K\langle X\rangle/\langle \operatorname{lm}_\sigma(I)\rangle$. We have

$$2 = \operatorname{GKdim}(A_{\operatorname{lm}\tau}) \leq \operatorname{GKdim}(A) = \operatorname{GKdim}(A_{\operatorname{lm}\sigma}) = \infty.$$

Based on Theorem 5.22, we will now propose a new algorithm to compute the GK-dimension of $K\langle X\rangle/I$.

In general, the construction of the Ufnarovski graph does not allow multiple edges, that is for every two vertices v, v' there is at most one edge from v to v'. There is however one exception, that is if $M \subseteq X$, then it is easily seen that ε is the only vertex in the Ufnarovski graph of M and there are $|X \setminus M|$ loops on

ε. Consider for example $K\langle x, y, z\rangle$ and the subset $M = \{x\} \subset \{x, y, z\}$. Then the Ufnarovski graph of M is given by



Since it is easier to work with graphs that do not have multiple edges, this case will be handled separately in the algorithm to compute the GK-dimension.

In the following algorithm and its subprocedure, $G \subset K\langle X\rangle \setminus \{1\}$ is a non-empty reduced finite Gröbner basis, $\Gamma = (V, E)$ is a graph (without multiple edges), $v \in V$ is a vertex, *path* is a route in Γ and with () we denote the empty route, *visited* and *cyclic* are subsets of V and *cache* is a dictionary where V is the set of keys and the associated values are in $\mathbb{N} \cup \{\text{NULL}, \infty\}$.

Let I be the ideal generated by G. If G is a Gröbner basis with respect to a length-compatible monomial ordering, or if the GK-dimension of $K\langle X\rangle/I$ is either 0 or infinite, then the Gelfand-Kirillov dimension algorithm returns the exact GK-dimension of $K\langle X\rangle/I$. Otherwise the algorithm returns a lower bound for the GK-dimension of $K\langle X\rangle/I$.

Algorithm 7 Gelfand-Kirillov dimension algorithm

```
procedure GelfandKirillovDimension(G)
    G ← lm(G)
    if G ⊆ X and |X \ G| > 1 then
        return ∞
    Γ ← the Ufnarovski graph of G
    cache ← cache[v] = NULL for all v ∈ V
    cycles ← 0
    for v ∈ V do
        cache ← CountCycles(Γ, v, (), ∅, ∅, cache)
        if cache[v] = ∞ then
            return ∞
        if cache[v] > cycles then
            cycles ← cache[v]
    return cycles
```

The cycle counting procedure recursively updates and returns the *cache* variable such that *cache*$[v]$ is ∞ if and only if from v there are two distinct cycles with a common vertex or a cycle containing a vertex from *cyclic* reachable in Γ. Otherwise *cache*$[v]$ is the maximal number of distinct cycles occurring in a single route starting at v in Γ. It is assumed that the initial call to the procedure is made as in Algorithm 7.

Note that all arguments are "copy-by-value", that is each call of the procedure has its own copies of the arguments.

Cycle counting procedure

```
procedure CountCycles(Γ, v, path, visited, cyclic, cache)
    if cache[v] ≠ NULL then
        return cache
    visited ← visited ∪ {v}
    path ← path with v appended
    cycles ← 0
    for (v, w) ∈ E do
        if w ∉ visited then
            cache ← CountCycles(Γ, w, path, visited, cyclic, cache)
            if cache[w] = ∞ then
                cache[v] ← ∞
                return cache
            if cache[w] > cycles then
                cycles ← cache[w]
        else
            cycle ← the subroute v_0, ..., v_m in path, where v_0 = w and v_m = v
            v_{m+1} ← v_0 ∈ cycle
            for v_i ∈ cycle do
                if v_i ∈ cyclic then
                    cache[v] ← ∞
                    return cache
                cyclic ← cyclic ∪ {v_i}
                E ← E \ {(v_i, v_{i+1})}
            for v_i ∈ cycle do
                cache ← CountCycles(Γ, v_i, path, visited, cyclic, cache)
                if cache[v_i] = ∞ then
                    cache[v] ← ∞
                    return cache
                if cache[v_i] + 1 > cycles then
                    cycles ← cache[v_i] + 1
    cache[v] ← cycles
    return cache
```

A visualization of the cycle counting procedure can be found in Example B.1 and Example B.2.

We would like to mention that Victor Ufnarovski provided a different algorithm to compute the growth of the Ufnarovski graph in [Ufn95] (Section 5.9).

5.3 Computing the K-dimension

Let $I \subset K\langle X\rangle \setminus \{1\}$ be an ideal and suppose $K\langle X\rangle/I$ is finite-dimensional as a vector space, that is the GK-dimension of $K\langle X\rangle/I$ is 0. We are interested in the K-dimension of $K\langle X\rangle/I$.

By Proposition 3.19, we know that the K-dimension of $K\langle X\rangle/I$ is the number of words that are normal modulo I. A naive approach to compute the K-dimension of $K\langle X\rangle/I$ would be to simply count all words that are normal

modulo I. To decide whether a word is normal modulo I we need a finite Gröbner basis of I.

Lemma 5.24 ([Xiu12, Proposition 6.3.8])**.** *Let I be an ideal of $K\langle X\rangle$ and let G be the reduced Gröbner basis of I. If $K\langle X\rangle/I$ is finite-dimensional as a vector space, then G is finite.*

Proof. We show the contraposition, therefore suppose the reduced Gröbner basis G of I is infinite. Since every subword of each word in $\mathrm{lm}(G)$ is normal modulo I and $\mathrm{lm}(G)$ contains infinitely many elements, it follows that there are infinitely many words that are normal modulo I. Then, by Proposition 3.19, $K\langle X\rangle/I$ is infinite-dimensional as a vector space. □

Algorithm 8 Naive K-dimension algorithm

Given the reduced finite Gröbner basis G of I, we can compute the K-dimension of $K\langle X\rangle/I$ as follows:

1. $M_0 \coloneqq \{\varepsilon\}, \quad i \coloneqq 0$
2. $M_{i+1} \coloneqq \{wx \mid w \in M_i,\, x \in X,\, wx \text{ is normal modulo } G\}$
3. If $M_{i+1} \neq \emptyset$, increment i by one and go to step 2.
4. Return $\sum |M_i|$.

We can use an *adjacency matrix* of the Ufnarovski graph to obtain a superior algorithm to compute the K-dimension of $K\langle X\rangle/I$.

Definition 5.25. Let $\Gamma = (V, E)$ be a graph and assume without loss of generality that $V = \{v_1, \ldots, v_n\}$. An *adjacency matrix* of Γ is a matrix $B \in \mathbb{N}^{n\times n}$ where the $(i,j)^{\text{th}}$ entry $b_{i,j}$ is 1 if and only if there is an edge from v_i to v_j in Γ and 0 otherwise.

The following Lemma is a well know property of an adjacency matrix, a proof can be found, for example, in [Xiu12] (Lemma 6.3.19).

Lemma 5.26. *Let $\Gamma = (V, E)$ be a graph, assume without loss of generality that $V = \{v_1, \ldots, v_n\}$ and let B be an adjacency matrix of Γ. The $(i,j)^{th}$ entry $b_{i,j}^{(m)}$ of B^m is the number of routes of length m from v_i to v_j for all $m \in \mathbb{N}$ and all $v_i, v_j \in V$.* □

In the following algorithm, let G be the reduced finite Gröbner basis of I and let $b_{i,j}^{(m)}$ denote the $(i,j)^{\text{th}}$ entry of the matrix B^m.

Algorithm 9 K-dimension algorithm

procedure KDIMENSION(G)
  $G \leftarrow \mathrm{lm}(G)$
  $s \leftarrow \min\{|w| : w \in G\}$
  $l \leftarrow \max\{|w| : w \in G\} - 1$
  $n \leftarrow \sum_{i=0}^{s-1} |X|^i$
  $n \leftarrow n + \sum_{i=s}^{l} |M_i|$ with $M_i = \{w \in \langle X\rangle \mid w \text{ is normal modulo } G,\ |w| = i\}$
  $B \leftarrow$ an adjacency matrix of the Ufnarovski graph of G
  $m \leftarrow 1$
  while B^m is not the zero matrix **do**
    $n \leftarrow n + \sum_{i,j} b_{i,j}^{(m)}$
    $m \leftarrow m + 1$
  return n

Proposition 5.27. *Algorithm 9 returns the K-dimension of $K\langle X\rangle/I$.*

Proof. Since all words of length less than s are normal modulo G, the number of words of length less than s that are normal modulo G is given by $\sum_{i=0}^{s-1} |X|^i$. By definition, $\sum_{i=s}^{l} |M_i|$ is the number of words of length greater than or equal to s and less than or equal to l that are normal modulo G. By Lemma 5.26, $\sum_{i,j} b_{i,j}^{(m)}$ is the number of routes of length m in the Ufnarovski graph of G and by Lemma 5.18 this is the number of words of length $l + m$ that are normal modulo G. Then it is clear that the final value of n is the number of all words that are normal modulo G and by Proposition 3.19 this is the K-dimension of $K\langle X\rangle/I$. □

Remark. The idea of using $\sum_{i,j} b_{i,j}^{(m)}$ to compute the number of words of length $l + m$ that are normal modulo G has already been used in [Xiu12, Theorem 6.3.27]. We have further improved the algorithm by using $|X|^i$ to compute the number of words of length $i < s$ that are normal modulo G.

The computations in Algorithm 9 are mainly numeric and those computations are generally much faster than the symbolic computations in Algorithm 8. Therefore Algorithm 9 is an improvement over Algorithm 8.

Bibliography

[Alu06] Gareth Alun Evans. *Noncommutative Involutive Bases*. PhD thesis, 2006. URL `https://arxiv.org/abs/math/0602140`.

[Ber78] George M. Bergman. The diamond lemma for ring theory. *Advances in Mathematics*, 29(2):178 – 218, 1978.

[BK76] Walter Borho and Hanspeter Kraft. Über die Gelfand-Kirillov-dimension. *Mathematische Annalen*, 220:1–24, 1976.

[BO93] Ronald V. Book and Friedrich Otto. *String-Rewriting Systems*. Springer-Verlag, 1993.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Leopold-Franzens-Universität Innsbruck, 1965.

[Buc85] Bruno Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. *Multidimensional systems theory*, 1985.

[KL99] Gunter R. Krause and Thomas H. Lenagan. *Growth of Algebras and Gelfand-Kirillov Dimension (Graduate Studies in Mathematics)*. American Mathematical Society, 1999.

[Li11] Huishi Li. *Gröbner Bases In Ring Theory*. World Scientific Publishing Company, 2011.

[LSL09] Roberto La Scala and Viktor Levandovskyy. Letterplace ideals and non-commutative Gröbner bases. *Journal of Symbolic Computation*, 44(10):1374–1393, 2009.

[LSL13] Roberto La Scala and Viktor Levandovskyy. Skew polynomial rings, Gröbner bases and the letterplace embedding of the free associative algebra. *Journal of Symbolic Computation*, 48:110–131, 2013.

[MN05] Jonas Månsson and Patrik Nordbeck. A generalized Ufnarovski graph. *Applicable Algebra in Engineering, Communication and Computing*, 16(5):293–306, Nov 2005.

[Mor86] Ferdinando Mora. Gröbner bases for non-commutative polynomial rings. In *Proceedings of the 3rd International Conference on Algebraic Algorithms and Error-Correcting Codes*, AAECC-3, pages 353–362, London, UK, 1986. Springer-Verlag.

[Mor94] Teo Mora. An introduction to commutative and noncommutative Gröbner bases. *Theoretical Computer Science*, 134(1):131 – 173, 1994.

[Mor16] Teo Mora. *Solving Polynomial Equation Systems IV*, volume 4 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2016.

[Nor01a] Patrik Nordbeck. *Canonical Bases for Algebraic Computations*. PhD thesis, Lund University, 2001.

[Nor01b] Patrik Nordbeck. On the finiteness of Gröbner bases computation in quotients of the free algebra. *Applicable Algebra in Engineering, Communication and Computing*, 2001.

[Rei98] Birgit Reinert. *Observations on Coset Enumeration*. Reports on Computer Algebra. Technische Universität Kaiserslautern, Fachbereich Mathematik, 1998.

[Sim94] Charles C. Sims. *Computation with Finitely Presented Groups*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1994.

[Stu13] Grischa Studzinski. *Implementation and applications of fundamental algorithms relying on Gröbner bases in free associative algebras*. PhD thesis, RWTH Aachen, 2013.

[Ufn82] V. A. Ufnarovski. A growth criterion for graphs and algebras defined by words. *Mathematical notes of the Academy of Sciences of the USSR*, 31(3):238–241, Mar 1982.

[Ufn95] V. A. Ufnarovskij. Combinatorial and asymptotic methods in algebra. In *Algebra VI. Combinatorial and asymptotic methods of algebra. Non- associative structures. Transl. from the Russian by R. M. Dimitrić*, pages 1–196. Berlin: Springer-Verlag, 1995.

[Xiu12] Xingqiang Xiu. *Non-commutative Gröbner Bases and Applications*. PhD thesis, Universität Passau, 2012.

Appendix A

Example Computations

All examples were executed on a Debian GNU/Linux machine with an i7-7700K CPU and 32 GiB of memory. We have used Singular 4.1.2 and GNU Time 1.9.

Example A.1. The goal is to compare the performance of the right FG-basis computation via Algorithm 6 with the right FG-basis computation via the two-sided Gröbner basis algorithm and a tag variable.

Take the degree right lexicographic ordering with $x \succ y$ as the ordering on $\mathbb{Q}\langle x, y\rangle$. Let Q be a Gröbner basis of $\langle xxx - yyy\rangle \subset \mathbb{Q}\langle x, y\rangle$ and let $F = \langle xxy - yxy,\ xx - y,\ yyy - y\rangle \subset \mathbb{Q}\langle x, y\rangle$. Even though there exists no finite right FG-basis of the right ideal generated by F in $\mathbb{Q}\langle x, y\rangle/\langle Q\rangle$, we can still compute a part of the right FG-basis.

To test the performance of Algorithm 6, we have created the test file `FG-basis.tst` with the following content:

```
LIB "freegb.lib";
ring r = 0,(x,y),dp;
ring R = freeAlgebra(r, 24);      // Letterplace ring
ideal Q = twostd(x*x*x - y*y*y);
qring qr = Q;                     // factor algebra
ideal F = x*x*y - y*x*y, x*x - y, y*y*y - y;
rightstd(F);
```

The computation is performed in the Letterplace ring with degree bound 24. Executing

```
$ time Singular < FG-basis.tst
```

resulted in the following output:

```
_[1]=y*y-y
_[2]=y*x-y
_[3]=x*x-y
_[4]=x*y*y*y-y
_[5]=x*y*x*y*y*y-y

...
```

```
_[14327]=x*y*y*x*x*y*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*y
   ↪ *y-y
_[14328]=x*y*x*y*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*y
   ↪ *y-y
_[14329]=x*y*y*x*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*y
   ↪ *y-y
_[14330]=x*y*x*x*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*y
   ↪ *y-y
_[14331]=x*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*y
   ↪ *y-y
Auf Wiedersehen.
49.78user 0.19system 0:50.05elapsed 99%CPU (0avgtext+0
   ↪ avgdata 127792maxresident)k
0inputs+0outputs (0major+40633minor)pagefaults 0swaps
```

For space reasons we only showed the first and last five generators of the result and ↪ denotes a line wrap. According to the output generated by `time`, the execution took 50.05 seconds and 127 792 KiB ≈ 125 MiB of memory was used.

To test the performance of the approach with the tag variable we have created the test file `FG-basis-tag.tst` with the following content:

```
LIB "freegb.lib";
ring r = 0,(x,y,#),dp;            // # tag variable
ring R = freeAlgebra(r, 24 + 1); // + 1 tag variable
ideal Q = twostd(x*x*x - y*y*y);
ideal F = x*x*y - y*x*y, x*x - y, y*y*y - y;
F = #*F;
ideal FG = twostd(F + Q);
simplify(reduce(FG, Q), 2);       // "FG - Q"
```

This time, the computation is performed in the Letterplace ring with degree bound 25 because the tag variable increases the degree of each polynomial by one. Executing

```
$ time Singular < FG-basis-tag.tst
```

resulted in the following output:

```
_[1]=#*y*y-#*y
_[2]=#*y*x-#*y
_[3]=#*x*x-#*y
_[4]=#*x*y*y*y-#*y
_[5]=#*x*y*x*y*y*y-#*y

...

_[14327]=#*x*y*y*x*x*y*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y
   ↪ *y*y-#*y
_[14328]=#*x*y*x*y*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y
   ↪ *y*y-#*y
_[14329]=#*x*y*y*x*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y
   ↪ *y*y-#*y
```

```
_[14330]=#*x*y*x*x*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y
   ↪ *y*y-#*y
_[14331]=#*x*y*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y*x*x*y
   ↪ *y*y-#*y
Auf Wiedersehen.
418.80user 20.79system 10:46.34elapsed 68%CPU (0
   ↪ avgtext+0avgdata 31893644maxresident)k
277120inputs+0outputs (23172major+13197402minor)
   ↪ pagefaults 0swaps
```

Again, for space reasons we only showed the first and last five generators of the result. Except for the leading `#` variable, the result is the same. The output generated by `time` however now indicates that the execution took 10 minutes and 46 seconds and 31 893 644 KiB ≈ 30 GiB of memory was used.

As a side note, replacing the degree right lexicographic ordering with the degree left lexicographic ordering in this example, we get

```
_[1]=y*y-y
_[2]=y*x-y
_[3]=x*x-y
```

and

```
_[1]=#*y*y-#*y
_[2]=#*y*x-#*y
_[3]=#*x*x-#*y
```

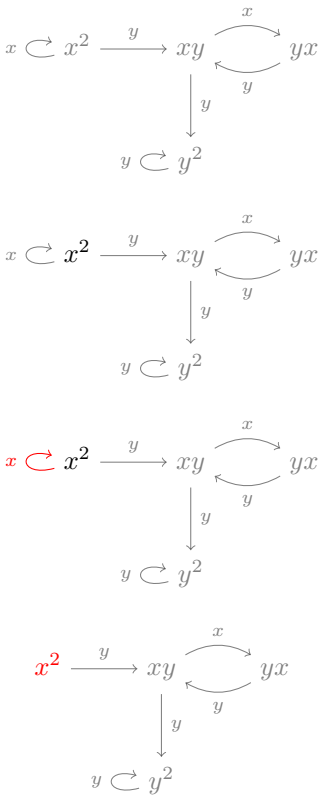
as the output. In this case $\{yy - y,\ yx - y,\ xx - y\}$ is a right FG-basis of F in $K\langle X\rangle/\langle Q\rangle$.

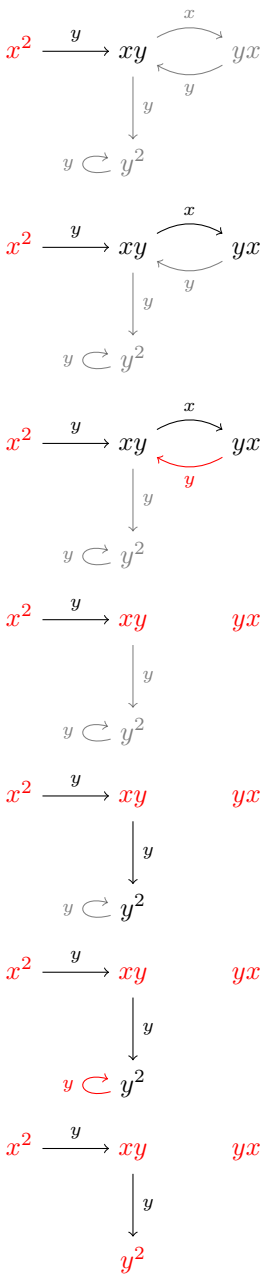
Appendix B

Cycle Counting Examples

Example B.1. What follows is a visualization of the steps of the cycle counting procedure in Algorithm 7. In this example a graph with a maximum of three distinct cycles in a single route is given as the input and the start vertex is x^2.

The visited vertices are black and the cyclic vertices are red. A red edge indicates that a new cycle has been found.

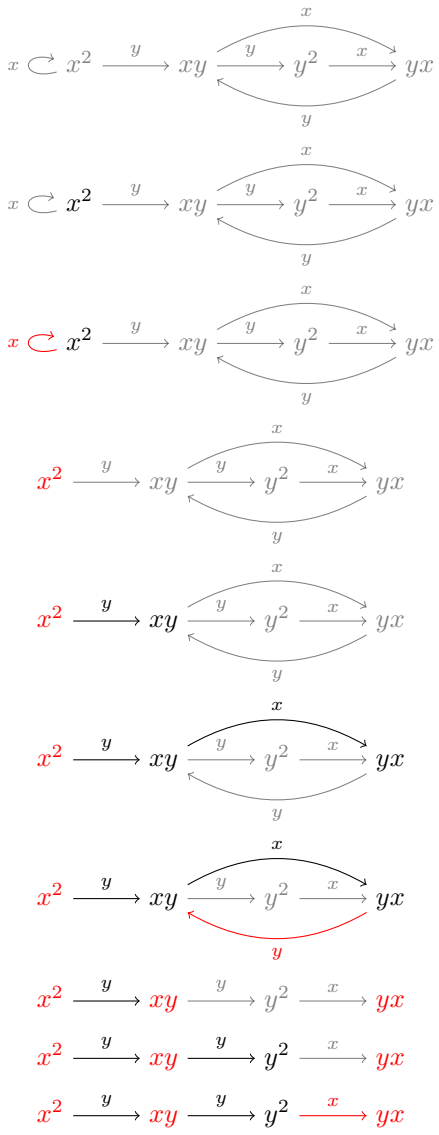




The vertices x^2, xy, y^2 are all part of distinct cycles. The route x^2, xy, y^2 connects the 3 cycles.

Example B.2. What follows is a visualization of the steps of the cycle counting procedure in Algorithm 7. In this example a graph with two intersecting cycles is given as the input and the start vertex is x^2.

The visited vertices are black and the cyclic vertices are red. A red edge indicates that a new cycle has been found.



There is an edge from y^2 to yx and thus a cycle involving the two vertices. But yx is already marked as cyclic (i.e. part of a different cycle), hence these are two intersecting cycles.