Implementation and Applications of Fundamental Algorithms relying on Gröbner Bases in Free Associative Algebras

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Mathematiker Grischa Studzinski aus Wuppertal

Berichter:
Prof. Dr. Eva Zerz, Prof. Dr. Martin Kreuzer

Tag der mündlichen Prüfung: 18.10.2013

Summary

In 2009, La Scala and Levandovskyy introduced a new approach for the computation of Gröbner bases of graded ideals in the free associative algebra. The approach utilizes so-called letterplace correspondence and thus the computations take place over a commutative polynomial ring. The latter is very important for applied computer algebra, since data structures and algorithms have been intensively studied in the last 50 years by numerous people. In 2012, La Scala presented the generalized letterplace correspondence for general, not necessarily graded ideals, where the homogenization was used.

In this thesis, an alternative approach has been studied, with the aim of direct computations, which do not use homogenization and thus are more effective and less complex. At first, the explicit isomorphism of the free associative algebra to a subalgebra of letterplace ring, equipped with the nonstandard multiplication is given. This lies in the heart of further constructions, data structures, algorithms and implementation. Moreover, the very important question on the presentation of monomial ordering for the free algebra is addressed. The embedding into letterplace ring allows the partial use of Robbiano's Theorem in the latter, resulting in the partial classification of orderings, in particular also of elimination orderings.

The images of ideals of the free algebra in the letterplace ring have additional structure, being shift-invariant. The new data structure was developed in order to encode an infinite orbit under the action of the shift via the single element and to transfer the fundamental operations into the new setting. Based on this data structure, the algorithms for the computation of a two-sided Gröbner basis of an ideal and of a left Gröbner basis of a left ideal in a finitely presented algebra were designed. Both algorithms are not using homogenization and can be applied to arbitrary ideals. Moreover, algorithms, important in applications, such as the computations of elimination, syzygies, Gel'fand-Kirillov dimension and the upper bound for the global homological dimension were considered and implemented.

The data structures and the Gröbner basis algorithms, mentioned above, were thoroughly implemented in the kernel of computer algebra system Singular. The implementation was extensively tested and compared to all major computer algebra systems, featuring similar functionality. The comparison demonstrated, that the implementation competes with and sometimes outperforms the fastest systems available. Further applied algorithms were implemented in Singular libraries.

The implemented tools were applied to numerous problems, ranging from group

theory (word problem and conjugator search problem for given elements in a given finitely presented group as well as the question of the finiteness of the latter group) with interest towards cryptography to the design of new generalized inverses in monoids (due to Drazin). Moreover, the state-of-the-art concerning the applications of generic tools like Gröbner bases to some important open problems in computational theory of finitely presented groups is established.

Zusammenfassung

In 2009 stellten La Scala und Levandovskyy einen neuen Weg zur Berechnung von Gröbnerbasen graduierter Ideale in der freien, assoziativen Algebra vor. Dieser Ansatz benutzt die sogenannte Letterplace Korrespondenz und deswegen werden die Berechnungen über einen kommutativen Polynomring ausgeführt. Dieser ist äußerst wichtig für angewandte Computeralgebra, da Datenstrukturen und Algorithmen in den letzten 50 Jahren von zahlreichen Wissenschaftlern intensiv studiert wurden. 2012 präsentierte La Scala die verallgemeinerte Letterplace Korrespondenz für allgemeine, nicht zwingend graduierte Ideale vor, wobei Homogenisierung benutzt wurde.

In dieser Arbeit wurde ein alternativer Weg untersucht, mit dem Ziel, direkte Berechnungsverfahren zu entwickeln, welche nicht Homogenisierung nutzen und deswegen effektiver und weniger komplex sind. Zunächst wird ein expliziter Isomorphismus zwischen der freien, assoziativen Algebra und einer Unteralgebra des Letterplace Ringes, welche versehen ist mit einer alternativen Multiplikation, angegeben. Dieser Isomorphismus liegt allen weiteren Konstruktionen, Datenstrukturen, Algorithmen und Implementationen zu Grunde. Darüber hinaus wird die wichtige Frage nach einer Darstellung von Monomordnungen für die freie, assoziative Algebra angesprochen. Die Einbettung in den Letterplace Ring erlaubt eine teilweise Nutzung des Satzes von Robbiano, wodurch eine partielle Klassifikation der Ordnungen, insbesondere von Eliminationsordnungen, möglich ist.

Die Bilder der Ideale der freien Algebra im Letterplace Ring haben zusätzliche Struktur, denn diese sind shift-invariant. Eine neue Datenstruktur wurde entwickelt, um die unendliche Bahn unter der Shift-Operation mittels eines Elementes darzustellen und um fundamentale Prozeduren in diese neue Situation zu übertragen. Basierend auf dieser Datenstruktur wurden die Algorithmen für die Berechnung einer zwei-seitigen Gröbnerbasis eines Ideals und einer Links-Gröbnerbasis eines Links-Ideals in einer endlich präsentierten Algebra gestaltet. Beide Algorithmen benutzen keine Homogenisierung und können auf beliebige Ideale angewendet werden. Weiterhin wurden weitere Algorithmen, welche für wichtige Anwendungen wie Berechnung von Elimination, Syzygien, Gel'fand-Kirillov Dimension und eine obere Schranke der globalen Dimension benutzt werden, betrachtet und implementiert.

Die oben erwähnte Datenstruktur und der Gröbnerbasen Algorithmus wurden sorgfältig in der Kern des Computeralgebra Systems SINGULAR implementiert. Das Programm wurde dann intensiv getestet und mit anderen wichtigen Computeralgebra Systemen verglichen. Dieser Vergleich zeigte, dass die Implementation

mit den anderen Systemen mithalten und in einigen Fällen sogar übertreffen kann. Die weiteren Algorithmen wurden in SINGULAR Bibliotheken implementiert.

Diese neuen Verfahren wurden auf zahlreiche Probleme, reichend vom Bereich der Gruppentheorie (Wort-Problem, Konjugator-Such-Problem für gegebene Elemente einer gegebenen endlich präsentierten Gruppe, sowie die Frage nach der Endlichkeit dieser Gruppe) unter Berücksichtigung kryptographischer Fragestellungen bis hin zur Gestaltung neuer, verallgemeinerter Inversen in Monoiden (gegeben durch Drazin), angewendet. Darüber hinaus wird der Stand der Dinge bezüglich der Anwendbarkeit von generischen Methoden wie Gröbnerbasen auf einige wichtige Probleme der Berechnungen von endlich präsentierten Gruppen neu definiert.

Introduction

Any finitely generated associative algebra can be presented as a factor of the free associative algebra. Therefore computations in the free algebra have many applications in different areas of mathematics, like cryptography, ring theory, homological algebra, representation theory of monoids, groups and algebras, algebraic system and control theory, quantum algebras, in mathematical and theoretical physics.

Many of those computations rely on Gröbner bases, that is a Gröbner basis is needed as input for an algorithm or at some point during the computations a Gröbner basis must be computed.

In theory the question of Gröbner bases computations was studied since the early years of computer algebra: Mora ([Mor86, Mor88, Mor94]), E. Green ([Gre93, Gre00]), Ufnarovskij ([Ufn95, Ufn98]) and Cojocaru et al. ([CPU99]) presented different facets of what we call today non-commutative Gröbner basis theory. In particular Mora discussed free non-commutative algebras and their quotient rings endowed also with negative (non-well-)orderings. and further extended this theory. Other important contributions were made by Apel and Lassner ([AL88]), moreover Apel further extended the theory in [Ape00].

In the last years there has been more progress in theoretical, implementational and practical directions. Notably, the interest in free associative algebras grew stronger, as indicated by e. g. the book of D. Green ([Gre03]), where the author considers also negative (non-well-)orderings for certain non-commutative cases with a very different motivation and meaning, compared to the theory of Mora ([Mor88]) and Apel ([Ape00]) and with the commutative case as in Greuel et al. ([GP08]). Evans and Wensley investigated in [EW07] involutive bases in non-commutative algebras.
Computer algebra systems like Magma [BCP97] and GAP [GAP13] now include packages which allow the user to compute Gröbner bases over the free algebra. However, there is less progress towards applications of these Gröbner bases. Notably, Xiu, under the supervision of Kreuzer, implemented a variety of algorithms for ApCoCoA which can be used for the most common applications of Gröbner bases ([Xiu12]).

With the recent work of La Scala and Levandovskyy [LL09] a new way to compute Gröbner bases emerged, where non-commutative Gröbner bases of graded ideals in free algebras are computed via the *letterplace correspondence*. The most im-

portant point for practical computer algebra is that the computations take place in a commutative ring, where the data structures as well as many fundamental algorithms have been deeply studied and enhanced in the past 40 years. Using homogenization La Scala generalized this approach to the case of non-graded ideals ([Sca12]).

In this work we continue this research direction and present novel ideas, supported by an implementation, for effective computations with general non-graded ideals in the free algebra by utilizing the generalized letterplace correspondence. In particular, we provide a direct algorithm to compute Gröbner bases of non-graded ideals. Surprisingly we realize its behavior as "homogenizing without a homogenization variable". Moreover, we develop new shift-invariant data structures for this family of algorithms and discuss them.

The computations of Gröbner bases rely heavily on the choice of an ordering. For the commutative case there is a classification of term orderings due to Robbiano ([Rob85]). In the non-commutative case however there is no such classification and most works simply assume that there exists a good ordering, which is true for the most situations. The lack of such a classification motivated us to study orderings and we came up with an efficient way to represent *good* orderings using the letterplace ring.

There are many applications for the computation of Gröbner bases and many of these problems, for instance as collected in the famous Kourovka Notebook (cf. [MK02]) fall into one of the following categories: determine whether a given presentation defines a finite or infinite group, solve the (generalized) word problem, solve the conjugator search problem, or solve the isomorphism problem. All these questions can be readily formulated in the monoid ring (or the group ring) corresponding to the given presentation. Most of them boil down to computing a single (one- or two-sided) Gröbner basis. As shown in [KB07], the conjugator search problem corresponds to the computation of a certain two-sided syzygy module.
These results have important applications in cryptography. Since the computational hardness of certain computations in finitely presented groups has been at the core of several proposals for non-commutative cryptosystems (see for instance [AAG99], [KLC+00] and the proposals in [GGK+06]), it is important to examine the feasibility of a straightforward attack via computing a non-commutative Gröbner basis.

Here we present the methods, based on the letterplace approach, which can be used to study those problems.

Gröbner basics were coined by Buchberger and Sturmfels to denote the most fundamental applications of Gröbner bases. In this work we concentrate on elimination, syzygies and left Gröbner bases in factor algebras. Notably, Gröbner basics were also recently studied by Xiu ([Xiu12]).

Acknowledgments

There are many people I would like to thank for their support.
First of all I would like to thank the German Research Foundation for the financial support which made the whole project possible.

Then of course I would like to thank my supervisor Dr. Viktor Levandovskyy who proposed the project to me, believed in and encouraged me and taught me a lot. Working with Viktor was always fun, even if there was more work than time available.

My sincere thanks go to Prof. Dr. Eva Zerz and Prof. Dr. Martin Kreuzer for their support and for the possibility to write this thesis. It was always a pleasure working for them and I count myself lucky to be part of their respective workgroups.

During the project I many interesting people from the computer algebra community. In my experience they are all really nice and I had many interesting and fruitful discussions for which I am very thankful, especially Roberto La Scala, who gave me new insights into the letterplace ring.
It was a great delight to personally meet Victor Ufnarovskij, who is not only a brilliant mind, but also one of the kindest person I ever met.

I am deeply grateful to the whole SINGULAR team who believed in the letterplace approach and allowed to include our methods into SINGULAR. Especially the mailing list and Dr. Hans Schönemann were very helpful towards any question related to the SINGULAR kernel.

Of course I would like to thank my colleagues in Aachen as well as in Passau for the many discussions, the help with problems which were not always related to work and for making working on the project really fun. I would like to mention two of them especially: Benjamin Schnitzler, without whom the implementation in SINGULAR would not be possible, and Daniel Andres, who was my colleague from the very beginning when I started my diploma thesis and who knows the answer to absolutely every question regarding LaTeX.

Last but not least I like to mention my family and my friends, who supported me throughout the project and accepted my escape from the social life especially during the last phase of the work.

Contents

1 Basic Structures

In this chapter we will briefly present the basic structures we are dealing with as well as lay down some notations. Then we will discuss the notion of orderings for the free algebra which will lead to the theory of Gröbner bases.

1.1 Monoids, Groups and Rings

In the first section we present notations and basic structures which are the theoretical layout for our work. While most of this should be known to the reader we like to introduce the setup which will be needed in a later chapter when the applications of this work are discussed.

1.1 Definition. Let M be a set.

- If there is a map $\cdot : M \times M \to M$ satisfying $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in M$ then $(M, \cdot)$ is called a *semi-group*.
- If in addition there is an element $e \in M$ such that $e \cdot a = a \cdot e = a \quad \forall a \in M$ then $(M, \cdot)$ is called a *monoid*.
- A monoid $(M, \cdot)$ is called *group* if for any element $a \in M$ there is an element $a^{-1} \in M$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

1.2 Remark. Often one refers to $\cdot$ as multiplication and the sign is omitted whenever there is no confusion possible. For simplicity we often identify M with $(M, \cdot)$. Let M be a monoid.

- M is called *commutative* or *abelian* if $ab = ba$ holds for all $a, b \in M$.
- An element $a \in M$ is called *unit* if there exists $b \in M$ such that $ab = ba = e$. The element b is called the *inverse* of a. If only $ab = e$ holds we call b a *right inverse* and a *right invertible*.

Of course one can also introduce the notion of *left invertible* when $ba = e$ holds.

1.3 Definition. Let M be a monoid.

- A subset $N \subseteq M$ is called a *submonoid* of M if $e \in N$ and $ab \in N \quad \forall a, b \in N$.

- A subset $G \subseteq M$ is called *generating set* for the submonoid N of M if N is the smallest submonoid containing G. We write $N = \langle G \rangle$ and we have $N = \{g_1 g_2 \cdots g_k \mid g_i \in G, k \in \mathbb{N}\}$.

It is important to note that everything we state for monoids also holds for groups. The following example of a monoid will be at the center of our studies.

1.4 Definition. Let M be a group.

- A subset $N \subseteq M$ is called a *subgroup* of M if $e \in N$ and $ab^{-1} \in N \quad \forall a, b \in N$.

- A subset $G \subseteq M$ is called *generating set* for the subgroup N of M if N is the smallest subgroup containing G. Again, we write $N = \langle G \rangle$ and we have $N = \{g_1 g_2 \cdots g_k \mid g_i \in G, k \in \mathbb{N}\}$.

1.5 Example. Let $\mathbf{X}$ be a set and denote by $x_1, x_2, \ldots$ the elements of $\mathbf{X}$. By $\langle \mathbf{X} \rangle$ we denote the set of all *words* $x_{j_1} \cdots x_{j_k}$ in $\mathbf{X}$, including the empty word, denoted by 1. We define a multiplication on $\langle \mathbf{X} \rangle$ by *concatenation* of words. With the identity element 1 $\langle \mathbf{X} \rangle$ becomes a monoid, the so called *free monoid*.
For a word $w = x_{j_1} \cdots x_{j_k}$ we call k the *length* of w, denoted by $\mathtt{lg}(w)$.
For two words $w, w' \in \langle \mathbf{X} \rangle$ we call w' a *prefix* or *left-divisor* of w if $w = w'u$ for some $u \in \langle \mathbf{X} \rangle$ and *suffix* or *right-divisor* if $w = uw'$ for some $u \in \langle \mathbf{X} \rangle$. Finally, w' divides w, if there are $u, v \in \langle \mathbf{X} \rangle$ such that $w = uw'v$ and we write $w' \mid w$.
For a subset $S \subset \langle \mathbf{X} \rangle$ we call a word $w \in \langle \mathbf{X} \rangle$ *normal* with respect to S, if there is no $s \in S$ such that $s \mid w$.

1.6 Definition. Let M be a monoid and X be a set. A map $\cdot : M \times X \to X$ is called a *(left) action* if $(mn) \cdot x = m \cdot (n \cdot x) \quad \forall m, n \in M, x \in X$ and $1 \cdot x = x \quad \forall x \in X$. The set $M \cdot x := \{m \cdot x \mid m \in M\}$ is called the *orbit* of x.

Equivalently the notion of *right action* can be introduced.

1.7 Definition.

- Assume we have a set R equipped with two composition maps $+$ and $*$, such that $(R, +)$ is a group and $(R \setminus \{0\}, *)$ is a monoid. We call $(R, +, *)$ a *ring*, if we have $a*(b+c) = a*b+a*c$ and $(b+c)*a = b*a+c*a$. We refer to $+$ as addition and $*$ as multiplication and skip the multiplication sign whenever there is no confusion possible.

- Let $(R, +, *)$ be a ring. If $(R \setminus \{0\}, *)$ is an abelian group we call R a *field*.

- Let $(R, +, *)$ be a ring and $(M, \dot{+})$ be an abelian group. If $(R, *)$ is acting on M (from the left) such that $(r+s) \cdot m = r \cdot m \dot{+} s \cdot m \quad \forall r, s \in R, m \in M$ and $r \cdot (m_1 \dot{+} m_2) = r \cdot m_1 \dot{+} r \cdot m_2 \quad \forall r \in R, m_1, m_2 \in M$ then M is called a *R (left) module*.

- A R-module M is called a *R-algebra* if M itself is a ring.

1.8 Remark. One often calls the underlying set ring (module, monoid) if the composition does not need to be introduced or is clear from the context.
If the ring R acts from the right on the R-module M such that $m \cdot (r + s) = m \cdot r \dot{+} m \cdot s \quad \forall r, s \in R, m \in M$ and $(m_1 \dot{+} m_2) \cdot r = (m_1 \cdot r) \dot{+} (m_2 \cdot r) \quad \forall r \in R, m_1, m_2 \in M$ we call M a right module and if M is a left and a right module we call M a bi-module.

Assume we have a ring $(R, +, *)$. We can define the *opposite* ring $R^{opp} := (R, +, \star)$ by setting $a \star b = b * a$. Therefore, every right R-module M is a left R^{opp} module and a bi-module can be viewed as a $R \times R^{opp}$ left module.

1.9 Definition.

- Let $(M, \cdot)$ and $(N, *)$ be two monoids. A map $f : M \to N$ is called *monoid homomorphism* if $f(x \cdot y) = f(x) * f(y)\ \forall x, y \in M$ and $f(1_M) = 1_N$.
- A monoid homomorphism between two groups M and N is called *group homomorphism*.
- Let $(M, \dot{+}, \cdot)$ and $(N, +, *)$ be two rings. A map $f : M \to N$ is called *ring homomorphism* if it is a monoid homomorphism between $(M, \dot{+})$ and $(N, +)$ as well as between $(M, \cdot)$ and $(N, *)$.

If f is bijective, then its inverse f^{-1} is also a homomorphism and f is called an *isomorphism* in this case.

1.10 Definition. Let R be a ring and M be a R-module.

- A subset $S \subseteq R$ is called a *subring* of R, if $1_R, ab, a + b \in S \forall a, b \in S$ and S is a ring.
- A subset $N \subseteq M$ is called a *(left) submodule* of M, if N is a subgroup of M and $rn \in N\ \forall r \in R, n \in N$.
- A subset $I \subseteq R$ is called a *two-sided ideal*, if $sr, rs \in I\ \forall s \in I, r \in R$ and $(I, +)$ is a subgroup of $(R, +)$. An ideal I is called *proper*, if $I \neq R$.

Again, one can introduce the notion of right and bi-submodule as well as right and left ideals. Note that if R is viewed as a R-module than two-sided ideals are exactly the sub-bimodules of R and we can define left and right ideals accordingly. If I is an (two-sided) ideal in R we write $I \trianglelefteq R$.

1.11 Remark. We like to point out two special kinds of modules. Let M be a R-module.

- We call M a *free* module if there exists a generating set E for M such that for all finite subsets $\tilde{E} \subseteq E$ we have that $\sum_{e_i \in \tilde{E}} r_i e_i = 0$ implies $r_i = 0\ \forall i$.

- A R-module P is called *projective* if there is a free R-module M and another R-module N such that $M = P \oplus N$.

1.12 Remark. Let S be a submodule of the R-module M. Then we have an equivalence relation on M given by $a \sim b \Leftrightarrow a - b \in S$.

1.13 Definition. Let S be a submodule of the R-module M. Then the *factor module* M/S is defined by the equivalence relation given by S. The elements of M/S are the equivalence classes $[a] = \{a + b \mid b \in S\}$ and M/S is again a R-module.

This definition extends to algebras and rings and we call the corresponding structures factor algebra or factor ring respectively.

1.14 Definition. Given a monoid M and a field $\mathbb{K}$ we can define the *monoid ring* $\mathbb{K}M$ as the set of all formal sums $\{\sum_i a_i m_i \mid a_i \in \mathbb{K}, m_i \in M\}$. It is a $\mathbb{K}$-vector space via $k\sum_i a_i m_i = \sum_i (ka_i)m_i \ \forall k \in \mathbb{K}, (\sum_i a_i m_i) \in \mathbb{K}M$ and a ring via $(\sum_i a_i m_i)(\sum_j b_j n_j) = \sum_{i,j}(a_i b_j)(m_i n_j)$.

As an application of the structures and to conclude this section we present the free algebra which will be the main tool throughout this work.

1.1.1 The free associative algebra

From now on let $\mathbb{K}$ be an arbitrary field and $\langle \mathbf{X} \rangle$ be the free monoid in a countable numbers of generators, denoted by $x_1, \ldots, x_n, \ldots$.
We define the free algebra as the monoid ring

$$\mathbb{K}\langle \mathbf{X} \rangle := \{\sum_{i \in \mathbb{I}} \alpha_i m_i \mid \alpha_i \in \mathbb{K}, m_i \in \langle \mathbf{X} \rangle, \quad \mathbb{I} \text{ an arbitrary index set,}$$
$$\text{only finitely many } \alpha_i \neq 0\}$$

and call the elements of $\mathbb{K}\langle \mathbf{X} \rangle$ *polynomials* and the elements of $\langle \mathbf{X} \rangle$ embedded in $\mathbb{K}\langle \mathbf{X} \rangle$ together with the identity 1 *monomials*.

Note that everything we say about left ideals can be easily translated to right ideals.
Again, one can consider the *enveloping algebra* $\mathbb{K}\langle \mathbf{X} \rangle \otimes \mathbb{K}\langle \mathbf{X} \rangle^{op}$, where $\mathbb{K}\langle \mathbf{X} \rangle^{op}$ denotes the *opposite* algebra, that is, $\mathbb{K}\langle \mathbf{X} \rangle$ endowed with the multiplication $a * b = b \cdot a \ \forall a, b \in \mathbb{K}\langle \mathbf{X} \rangle$. Then $\mathbb{K}\langle \mathbf{X} \rangle$ is a $\mathbb{K}\langle \mathbf{X} \rangle \otimes \mathbb{K}\langle \mathbf{X} \rangle^{opp}$ module and the action of $\mathbb{K}\langle \mathbf{X} \rangle \otimes \mathbb{K}\langle \mathbf{X} \rangle^{opp}$ on $\mathbb{K}\langle \mathbf{X} \rangle$ is given by:

$$\mathbb{K}\langle \mathbf{X} \rangle \otimes \mathbb{K}\langle \mathbf{X} \rangle^{opp} \times \mathbb{K}\langle \mathbf{X} \rangle \ \to \ \mathbb{K}\langle \mathbf{X} \rangle : \ (l \otimes r, p) \mapsto l \cdot p \cdot r.$$

As an example we state a theorem which shows how the free algebra can be used to study general structures.

1.15 Proposition. Any finitely presented algebra A is isomorphic to a factor of the free algebra.

Proof: Say A is generated by $\{e_i \mid i \in S \subseteq \mathbb{N}\}$ and take $\mathbb{K}\langle \mathbf{X} \rangle$ in the same number of variables. Then one has a homomorphism $\phi : \mathbb{K}\langle \mathbf{X} \rangle \to A : x_i \mapsto e_i$ and the Homomorphism Theorem holds the claim. q.e.d.

This can be used to study many interesting rings, like group and monoid rings, and different kinds of algebras, like G-algebras or path algebras. We will see in a later chapter some of those examples. For now we show how a group can be represented as a factor of the free algebra.

1.16 Example. Consider a group G generated by $\{a_1, \ldots, a_n\}$. Moreover, assume G is finitely presented, so we have finitely many *relations* $\{r_1, \ldots, r_s\}$ on the generators. Consider the ring homomorphism $\phi : \mathbb{K}\langle x_1, \ldots, x_n \rangle \to \mathbb{K}G$. We then have $\mathbb{K}\langle \mathbf{X} \rangle / \ker(\phi) \cong \mathbb{K}G$. Since the group G itself forms a $\mathbb{K}$-basis of $\mathbb{K}G$ a $\mathbb{K}$-basis of $\mathbb{K}\langle \mathbf{X} \rangle / \ker(\phi)$ will represent the elements of the group.

1.2 Orderings

We now introduce orderings. While the definition works for (non-empty) sets in general, we will study orderings for the free algebra in detail.

1.17 Definition. An *(strict total) ordering* $<$ is a total, transitive and asymmetric relation on a non-empty set $\mathbf{X}$, that is

- If $a < b$ then $\neg(b < a)$ *(asymmetry)*;
- If $a < b$ and $b < c$ then $a < c$ *(transitivity)*;
- Either $a < b$ or $b < a \quad \forall a, b \in \mathbf{X}, a \neq b$ *(totality)*.

From now on let $\langle \mathbf{X} \rangle$ be a monoid with neutral element $1 \in \langle \mathbf{X} \rangle$.

1.18 Definition. A total ordering $<$ on $\langle \mathbf{X} \rangle$ is called a

- *well-ordering*, if every non-empty subset of $\mathbf{X}$ has a least element with respect to $<$.
- *reduction ordering* or compatible with multiplication, if for all $m_1, m_2, l, r \in \mathbf{X}$ with $m_1 < m_2$ we have $lm_1r < lm_2r$.
- *monomial ordering*, if it is a well-ordering and a reduction ordering. In particular, $1 < x \quad \forall x \in \mathbf{X}$.

Note that for a reduction ordering we have if $m, n \in \langle \mathbf{X} \rangle$ are such that n *divides* m, that is, if there exists $l, r \in \langle \mathbf{X} \rangle$ with $m = lnr$, denoted by $n \mid m$, then we have $n < m$, because for $1 < l, r \in \langle \mathbf{X} \rangle$ we have $n = 1n < ln = ln1 < lnr = m$.
With a given strict and total ordering on $\langle \mathbf{X} \rangle$ we can write each polynomial $f \in \mathbb{K}\langle \mathbf{X} \rangle \setminus \{0\}$ in the free algebra $\mathbb{K}\langle \mathbf{X} \rangle$ over $\langle \mathbf{X} \rangle$ uniquely as $f = \sum_{i=1}^{k} c_i m_i$, such that $c_i \in \mathbb{K} \setminus \{0\}$ and $m_i \in \langle \mathbf{X} \rangle$ with $m_1 < \cdots < m_k$.

1.19 Example. Let $\langle \mathbf{X} \rangle$ be the free monoid generated by $\{x_1, \ldots, x_n\}$ and assume that $x_1 < x_2 < \ldots < x_n$, so we have a so-called *linear preordering*.

- Let $\mu, \nu \in \langle \mathbf{X} \rangle \setminus \{1\}$, such that $\mu = x_{j_1} x_{j_2} \cdots x_{j_k},\ \nu = x_{l_1} x_{l_2} \cdots x_{l_{\tilde{k}}}$. Then we have:

$$\begin{aligned} \mu <_{\text{llex}} \nu \quad \Longleftrightarrow \quad & \exists 1 \leq i \leq \min\{k, \tilde{k}\} :\ x_{j_w} = x_{l_w}\ \forall w < i\ \wedge\ x_{j_i} < x_{l_i} \\ & \text{or } \nu = \mu\tilde{\nu} \quad \text{for some } \tilde{\nu} \in \langle \mathbf{X} \rangle. \end{aligned}$$

  This is called the *left lexicographical ordering*.
  Analogously one can define the *right lexicographical ordering*:

$$\begin{aligned} \mu <_{\text{rlex}} \nu \quad \Longleftrightarrow \quad & \exists 1 \leq i \leq \min\{k, \tilde{k}\} :\ x_{j_{k-w}} = x_{l_{\tilde{k}-w}} \\ & \forall w \text{ such that } \min\{k, \tilde{k}\} - w > i\ \wedge\ x_{j_i} < x_{l_i} \\ & \text{or } \nu = \tilde{\nu}\mu \quad \text{for some } \tilde{\nu} \in \langle \mathbf{X} \rangle. \end{aligned}$$

- Take μ, ν as before. We define:

$$\mu <_{\text{gradlex}} \nu \quad \Longleftrightarrow \begin{cases} k < \tilde{k} & \text{, or} \\ k = \tilde{k} \text{ and } \mu <_{\text{llex}} \nu. \end{cases}$$

  This is called the *graded* or *degree (left) lexicographical ordering*.

- Take $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{R}^n \setminus \{0\}$ and again let $\mu, \nu \in \langle \mathbf{X} \rangle$ as before.

$$\mu <_{\omega} \nu \quad \Longleftrightarrow \begin{cases} \sum_{i=1}^{k} \omega_{j_i} < \sum_{i=1}^{\tilde{k}} \omega_{l_i} & \text{or} \\ k = \tilde{k} \text{ and } \mu <_{\text{llex}} \nu. \end{cases}$$

  This is called the *weighted degree (lexicographical) ordering* with weight vector ω.

1.20 Remark. The degree lexicographical ordering is a monomial ordering and enjoys many nice properties.
The (left or right) lexicographical ordering is not a monomial ordering, in fact it is not even multiplicative: Take $\mathbb{K}\langle x, y \rangle$ with the left lexicographical ordering. Then we have $y^2 > y$, but $y^2 x < yx$. Nevertheless, the lexicographical ordering gives rise to many other orderings and for that it is of interest.

It is important to note that there are different meanings of the word degree, which are commonly confused with one another.

1.21 Definition. For a given ordering $<$ we define the *multi-degree* of a monomial $m = x_{i_1}^{k_1} \cdots x_{i_j}^{k_j}$ as the j-tuple $(k_1, \ldots, k_j)$ and the *total degree* as $\sum_{r=1}^{j} k_r$. If $<$ is a weighted degree ordering we also define the *weighted total degree* of m as $\sum_{l=1}^{j} \omega_{i_l} k_l$ and denote it by $\deg_\omega(m)$. Moreover, by $\deg_{x_i}(m)$ we denote the number of occurrences of x_i in m.
We define the *leading monomial* of a polynomial $f = \sum_{i=1}^{k} c_i m_i \neq 0$ as the maximum (with respect to $<$) of the set $\{m_i \mid c_i \neq 0\}$ and denote it by $\mathtt{lm}(f)$. Also we call the coefficient by $\mathtt{lm}(f)$ the *leading coefficient*, denoted by $\mathtt{lc}(f)$ and we define the *leading term* of f as $\mathtt{lt}(f) = \mathtt{lc}(f) \cdot \mathtt{lm}(f)$. The (total) degree of a polynomial f is defined to be the (total) degree of its leading monomial. We denote the total degree of f by $\mathrm{tdeg}(f)$ and the multi-degree by $\deg(f)$.
Finally we will denote with $\mathtt{L}(\langle G \rangle)$ the *leading ideal* of $\langle G \rangle$, which is the ideal of $\mathbb{K}\langle \mathbf{X} \rangle$ generated by the leading monomials of G.
Since $\mathbb{K}$ is a field there is no loss of generality to assume that all polynomials of a given generating set are monic, that is the leading coefficient equals 1.

1.22 Definition. Consider the elements of $\mathbb{K}\langle \mathbf{X} \rangle$ as elements of $\mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$. If $\mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$ is equipped with a monomial ordering $<$ we denote the *restriction* of $<$ on $\mathbb{K}\langle \mathbf{X} \rangle$by $<_{|\mathbf{X}}$. For $m, n \in \mathbb{K}\langle \mathbf{X} \rangle$ holds: $m <_{|\mathbf{X}} n \ :\Leftrightarrow \ m < n \ \forall m, n \in \mathbb{K}\langle \mathbf{X} \rangle$.

1.23 Lemma. If $<$ is a monomial ordering on $\mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$, then the restriction $<_{|\mathbf{Y}}$ of $<$ on $\mathbb{K}\langle \mathbf{Y} \rangle$ is again a monomial ordering.

Proof: By definition we have $m_1 <_{|\mathbf{Y}} m_2 \quad \Leftrightarrow \quad m_1 < m_2 \qquad \forall m_1, m_2 \in \langle \mathbf{Y} \rangle$, henceforth the properties of $<$ can be easily translated to $<_{|\mathbf{Y}}$. q.e.d.

As we will see in a later chapter, another important type of ordering are elimination orderings.

1.24 Definition. Let $\mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$ be a free algebra in the variables $\mathbf{X} = \{x_1, \ldots, x_n\}$ and $\mathbf{Y} = \{y_1, \ldots, y_m\}$. An ordering $<$ is called *elimination ordering* for $\mathbf{X}$ if $\forall f \in \mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle \setminus \{0\}$ the property $\mathtt{lm}(f) \in \langle \mathbf{Y} \rangle$ already implies $f \in \mathbb{K}\langle \mathbf{Y} \rangle \subset \mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$.

1.25 Lemma. Assume we have an elimination ordering $<$ for $\mathbf{X}$ on $\langle \mathbf{X}, \mathbf{Y} \rangle$, then we have $x > m \ \forall x \in \mathbf{X}, m \in \langle \mathbf{Y} \rangle$.

Proof: Take arbitrary $x \in \mathbf{X}$ and $m \in \langle \mathbf{Y} \rangle$. In order to fulfill the elimination property we have $\mathtt{lm}(x + m) = x$, since m is a monomial in $\langle \mathbf{Y} \rangle$. q.e.d.

1.26 Corollary. Let $\mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$ be as before and take an elimination ordering $<$ for $\mathbf{X}$. Then $x > y_{i_1} \cdots y_{i_r} \ \forall x \in \mathbf{X}, y_{i_j} \in \mathbf{Y}, \ 1 \leq j \leq r, r \in \mathbb{N}$.

In commutative algebra an easy way to obtain an elimination ordering is to introduce weights for the variables: those of $\mathbf{X}$ will have weight one and those of $\mathbf{Y}$ will have weight zero. However, in the non-commutative case this leads to a

ordering which is not a reduction ordering.
One way to get to a monomial ordering which has the elimination property is to start with a preordering and use the multiplication rule to expand it.

1.27 Example. Take $\mathbb{K}\langle x, y\rangle$ and say we want an elimination ordering for x. We know that $x > y^n \quad \forall n \in \mathbb{N}$ and $y^{n+1} > y^n$, the latter one being a consequence of multiplicativity.
Then we can extend $x > y^2 > y$ to

$$x^2 > \begin{Bmatrix} xy \\ yx \end{Bmatrix} > x > y^2 > y$$

using multiplicativity. In order to get a complete ordering for all monomials up to total degree 2 we have to choose either $xy > yx$ or $xy < yx$. For this example we choose $xy > yx$.
Applying left and right multiplication of the variables one more time we will get

$$x^3 > x^2y > xyx > yx^2 > x^2 > xy^2 > yxy > \begin{Bmatrix} xy \\ y^2x \end{Bmatrix} > yx > x > y^3 > y^2 > y.$$

So we have to choose whether $xy > y^2x$ or $y^2x > xy$, each choice giving us an elimination ordering up to total degree 3.
Continuing this procedure one has to make more choices, depending on the total degree (and in the general case on the number of variables). In a later chapter we will discuss the notion of a good representation for an ordering. For now we will just give two examples of a monomial elimination ordering.

- For $m_1, m_2 \in \langle \mathbf{X} \rangle$ we say $m_1 >_{\text{Elim}} m_2$ if we have $\deg_{x_i}(m_1) > \deg_{x_i}(m_2)$ for some $i \in \underline{n}$ and $\deg_{x_l}(m_1) = \deg_{x_l}(m_2) \forall l \in \{1, \ldots, i-1\}$ or $\deg_{x_i}(m_1) = \deg_{x_i}(m_2) \forall i \in \underline{n}$ and $m_1 >_{\text{llex}} m_2$. This ordering works similar to the lexicographical ordering that is for any chosen $j \in \mathbb{N}$ with $1 < j \leq n$ it is an elimination ordering for $x_j, \ldots, x_n$.

- For $m_1, m_2 \in \langle \mathbf{X}, \mathbf{Y} \rangle$ we say $m_1 >_{\text{elim}} m_2$ if we have $\deg_{\mathbf{X}}(m_1) > \deg_{\mathbf{X}}(m_2)$ or $\deg_{\mathbf{X}}(m_1) = \deg_{\mathbf{X}}(m_2)$ and $m_1 = lm_2r$ for some $l, r \in \langle \mathbf{X} \rangle$ or $\deg_{\mathbf{X}}(m_1) = \deg_{\mathbf{X}}(m_2)$, $m_1 \neq lm_2r$ for all $l, r \in \langle \mathbf{X} \rangle$ and $m_1 >_{\text{llex}} m_2$.

The first example corresponds to the choice $y^2x > xy$, while the second ensures that $xy > y^2x$.

Since we have chosen $1 < x$ for each variable x it is clear that $>_{\text{Elim}}$ and $>_{\text{elim}}$ are well orderings.
To see that these are indeed reduction orderings it is sufficient to check the condition for each variable $x \in \mathbf{X}$ and $x \in \{\mathbf{X} \cup \mathbf{Y}\}$ respectively. So assume we have $m_1, m_2 \in \mathbb{K}\langle \mathbf{X} \rangle$ with $m_1 >_{\text{Elim}} m_2$ and take $x_i \in \mathbf{X}$. Since multiplication

from left or right does not change the relation between $\deg_{x_i}(m_1)$ and $\deg_{x_i}(m_2)$ we only have to prove the claim in the case of $\deg_{x_i}(m_1) = \deg_{x_i}(m_2) \forall i \in \underline{n}$, which also implies $\text{tdeg}(m_1) = \text{tdeg}(m_2)$ and so the claim follows from fact that the degree lexicographical ordering is a reduction ordering. Note that we could change the second condition into $\deg_{x_i}(m_1) = \deg_{x_i}(m_2) \forall i \in \underline{n}$ and $m_1 >_{\text{gradlex}} m_2$ to get the exact same ordering.
For $<_{\text{elim}}$ the proof follows similarly.

Before we conclude this section with some very interesting examples of orderings we like to introduce the notion of gradings here.

1.28 Definition.

- A ring R is called *graded* if there is a decomposition into additive groups $R = \bigoplus_{i \in \mathbb{N}} R_i$ such that $r \in R_k, s \in R_j \Rightarrow rs \in R_{k+j} \quad \forall k, j \in \mathbb{N}$, that is $R_k R_j \subseteq R_{k+j}$. Elements of any factor R_i of the decomposition are known as *homogeneous* elements of degree i. An ideal $I \trianglelefteq R$ is called *homogeneous* if every element $p \in I$ is the sum of homogeneous elements that belong to I.

- Let R be a ring and A be a R-algebra. A *filtration* of A is an increasing sequence of subspaces $\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A$ such that $A = \bigcup_{i \in \mathbb{N}} A_i$ and $A_j A_k \subseteq A_{j+k} \quad \forall j, k \in \mathbb{N}$.

Note that each graded ring is also a filtered algebra.
It is easy to see that on the free algebra monomial orderings induce a grading whenever one has the notion of a (weighted) total degree. However, not every grading is induced by an ordering. We will need this in a later chapter.

To close this section we present an overview of some examples of orderings.

1.2.1 An overview on orderings

E.L. Green stated in [Gre96] that one of the problems with answering questions about universal Gröbner bases is that admissible orderings are not classified. In fact most works about non-commutative Gröbner basis theory do not focus on the question of orderings and it is often assumed that a *good* ordering exists and even monomial elimination orderings are not studied well.
While we do not intend to work on a complete classification we want to give an overview on some somehow unusual examples we encountered to encourage further studies.

1.29 Example. Assume we have the free algebra $\mathbb{K}\langle \mathbf{X} \rangle$ generated by n variables. We define an ordering inductively. For monomials $m_1, m_2 \in \mathbb{K}\langle x_1 \rangle$ we set $m_1 = x_1^{k_1} > m_2 = x_1^{k_2} \quad \Leftrightarrow \quad k_1 > k_2$. Let $1 < k \leq n$. Then every monomial $m \in \mathbb{K}\langle x_1, \ldots, x_k \rangle$ can be written as $m = m_1 x_k m_2 x_k \ldots x_k m_r$ with $m_i \in \mathbb{K}\langle x_1, \ldots, x_{k-1} \rangle$. Say $m = m_1 x_k m_2 x_k \ldots x_k m_r$ and $n = n_1 x_k n_2 x_k \ldots x_k n_l$

are two monomials. Then $m > n$ if $r > l$ or if $r = l$ and there exists j such that $m_i = n_i$ for $i > j$ and $n_j < m_j$.
This ordering can be used to present so called *G-algebras* as factors of the free algebra and was discovered by Mora and presented in [KRW90]. Examples for G-algebras include Weyl algebras and Ore extensions of associative rings (see for example [Lev05]).
Note that this ordering has also the elimination property and was studied in this regard in [BB98].

1.30 Example.
For $n \geq 2$ define $\mathcal{O}_n(\lambda_{ji})$ as the $\mathbb{K}$-algebra generated by $x_1, \ldots, x_n$ with the relations $x_j x_i = \lambda_{ji} x_i x_j, \quad \lambda_{ji} \in \mathbb{K}, \quad 1 \leq i \leq j \leq n$. We call $\mathcal{O}_n(\lambda_{ji})$ the *skew polynomial algebra*.
Obviously there is an canonical $\mathbb{K}$-algebra epimorphism $\pi : \mathbb{K}\langle \mathbf{X} \rangle \to \mathcal{O}_n(\lambda_{ji})$. For any given ordering $\prec$ on $\mathcal{O}_n(\lambda_{ji})$ we define a new ordering on $\mathbb{K}\langle \mathbf{X} \rangle$ by setting
$u <_{et} v$ if $\begin{cases} \pi(u) \prec \pi(v), & \text{or} \\ \pi(u) = \pi(v) & \text{and } u <_{lex} v \end{cases}$ for any two monomials $u, v \in \langle \mathbf{X} \rangle$.
We call $<_{et}$ the *lexicographic extension*. If $\prec$ is a monomial ordering on $\mathcal{O}_n(\lambda_{ji})$ then $<_{et}$ is a monomial ordering as well as proven in [Li12].
This ordering is used to determine the correlation between Gröbner bases in $\mathbb{K}\langle \mathbf{X} \rangle$ and $\mathcal{O}_n(\lambda_{ji})$. This examples gives rise to whole class of examples by extending orderings from other algebras to $\mathbb{K}\langle \mathbf{X} \rangle$, whenever there is an epimorphism.

1.31 Example. Consider a free algebra $A := \mathbb{K}\langle x_1, \ldots, x_n, y_1, \ldots, y_r \rangle$ in $n + r$ variables and take the set $A_{\leq d} := \mathbb{K}\langle x_1, \ldots, x_n, y_1, \ldots, y_r \rangle_{\leq d}$, that is the set of all polynomials with unweighted total degree less or equal than $d \in \mathbb{N}$.
Equip A with a weighted degree orderings, where the x_i get the weight $1000d$ and the y_i the weight 1. Because this is a positive weight ordering on A it is a well ordering, as stated before.
On $A_{\leq d}$ on the other hand this ordering behaves like an elimination ordering, since there is no monomial in $\mathbb{K}\langle y_1, \ldots, y_r \rangle_{\leq d}$ that is greater or equal to any monomial containing at least one x_i. This can be used to mimic an elimination ordering when a degree bound is applied. For a detail description we refer to [Tra07].

1.32 Example. Let $\mathbf{X}$ and $\mathbf{Y}$ be to disjoined sets of variables and consider $\mathbb{K}\langle \mathbf{X} \rangle$ and $\mathbb{K}\langle \mathbf{Y} \rangle$ equipped with monomial orderings $<_{\mathbf{X}}$ and $<_{\mathbf{Y}}$.
Suppose $u \in \langle \mathbf{X}, \mathbf{Y} \rangle$. Then u can be written as $u = a_0 b_1 a_1 b_2 \cdots a_{r-1} b_r a_r$, where $b_i \in \langle \mathbf{Y} \rangle$ and $a_i \in \langle \mathbf{X} \rangle$. Let $v \in \langle \mathbf{X}, \mathbf{Y} \rangle$ be another monomial and write it as $v = c_0 d_1 c_1 \cdots c_{s-1} d_s c_s$ corresponding to the decomposition before. Now we say
$u < v$ if $\begin{cases} b_1 \cdots b_r <_{\mathbf{Y}} d_1 \cdots d_s, & \text{or} \\ b_1 \cdots b_r = d_1 \cdots d_s & \text{and } (a_0, \ldots, a_r) <_{lex,\mathbf{X}} (c_0, \ldots, c_r), \end{cases}$
where $<_{lex,\mathbf{X}}$ is the lexicographic ordering on $(\langle \mathbf{X} \rangle)^{r+1}$ induced by $<_{\mathbf{X}}$. We call

$<_{\mathbf{X}} \wr <_{\mathbf{Y}} :=<$ the *wreath product ordering* of $<_{\mathbf{X}}$ and $<_{\mathbf{Y}}$.
Sims proved in [Sim94] that if $<_{\mathbf{X}}$ and $<_{\mathbf{Y}}$ are monomial orderings then so is $<_{\mathbf{X}} \wr <_{\mathbf{Y}}$.

1.3 Gröbner Bases

This section introduces the general theory of non-commutative Gröbner bases. We go along the lines of [Stu10], where a similar section was presented. We will omit some of the details here and refer the interested reader to the original source.

1.33 Definition. Let $G \subset \mathbb{K}\langle \mathbf{X} \rangle \setminus \{0\}$ and $\langle G \rangle =: I$. A *normal form* of $f \in \mathbb{K}\langle \mathbf{X} \rangle$ with respect to G is an element $g \in \mathbb{K}\langle \mathbf{X} \rangle$ such that $f - g \in I$ and either $g = 0$ or $\mathtt{lm}(g_i) \nmid \mathtt{lm}(g)\ \forall g_i \in G$. We denote a normal form of f with respect to G by $\mathtt{NF}(f, G)$.
A subset $G \subset I$ is called a *Gröbner basis of* I if the leading monomial of an arbitrary element in I is a multiple of the leading monomial of an element in G. Equivalently, G is a Gröbner basis if $\langle \{\mathtt{lm}(g) \mid g \in G\} \rangle = \mathtt{L}(I)$.

1.34 Remark. Note that a Gröbner basis always exists, since we can take $G = I \setminus \{0\}$. This is due to the fact that we do not demand our Gröbner basis to be finite. In fact there are some ideals, which do not posses a finite Gröbner basis. One can easily see the relevance of Gröbner bases: If G is a Gröbner basis of I then a normal form for $f \in I$ is given by 0 and this is the only choice we have. However, neither the normal form nor the Gröbner basis are unique in general. In order to get uniqueness we refine the definition a little bit.

1.35 Definition. A normal form $g = \sum_{i=0}^{k} a_i t_i, \quad a_i \in \mathbb{K},\ t_i \in \mathbf{X}$ of $f \in \mathbb{K}\langle \mathbf{X} \rangle$ with respect to G is called *reduced*, if g is monic, that is, its leading coefficient is 1, and if $\mathtt{lm}(g_w) \nmid t_i \quad \forall i = 0, \ldots, k,\ g_w \in G$. We often speak about *the* normal form.

Before we solve our uniqueness problem, let us see the general idea on constructing normal forms.

1.36 Definition. Let $\{g_i \mid i \in \mathbb{J}, \mathbb{J} \text{ an arbitrary index set}\} = G \subset \mathbb{K}\langle \mathbf{X} \rangle$ and $\langle G \rangle =: I$.

- Let $\tilde{\tau}_i : \mathbf{X} \to \mathbb{K}\langle \mathbf{X} \rangle$:
  $x \mapsto \begin{cases} A(\mathtt{lm}(g_i) - \mathtt{lc}(g_i)^{-1} g_i)B, & \text{if } x = A\mathtt{lm}(g_i)B \text{ for some } A, B \in \mathbf{X} \\ x & \text{otherwise} \end{cases}$
  and let $\tau_i : \mathbb{K}\langle \mathbf{X} \rangle \to \mathbb{K}\langle \mathbf{X} \rangle$ be the $\mathbb{K}$-linear continuation of $\tilde{\tau}$. One calls τ_i a *reduction* with g_i.

- Let $f \in \mathbb{K}\langle \mathbf{X} \rangle$. One says that τ_i acts *trivially* on f, if the coefficient of $A\mathtt{lm}(g_i)B$ is zero in f for all $A, B \in \mathbf{X}$. f is called *irreducible*, if all reductions act trivially on f.
  In other words $\tau_i(f) = f \; \forall i \in J$.

It is important to note that Gröbner bases are a special generating set.

1.37 Lemma. Let G be a Gröbner basis of a given ideal I. Then $I = \langle G \rangle$.

Proof: Since $G \subset I$ we have $\langle G \rangle \subset I$, so take $f \in I \setminus \langle G \rangle$ with minimal degree, that is $f := \min_{\deg(\tilde{f})} \{\tilde{f} \in I \setminus \langle G \rangle\}$ (the minimum exists because we assume that $<$ is a monomial ordering) and say without loss of generality that f is monic. By the definition of a Gröbner basis there exists $g \in G$ such that $\mathtt{lm}(g) \mid \mathtt{lm}(f)$, say $\mathtt{lm}(f) = A\mathtt{lm}(g)B$ for some $A, B \in \mathbf{X}$. Then $\tilde{f} = f - AgB \in I$ and $\deg(\tilde{f}) < \deg(f)$, so by minimality $\tilde{f} \in \langle G \rangle$. But then $f = AgB + \tilde{f} = AgB + \sum_{p \in P \subset \langle G \rangle} a_p p b_p \in \langle G \rangle$, which is a contradiction. q.e.d.

We now state an algorithm which allows one to compute normal forms with respect to an arbitrary set of polynomials. We will focus on the case that this set is a generating set, although this is not necessarily a requirement.

1.38 Algorithm.
Input: An ideal $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$ with a given generating set $G = \{g_i \mid i \in J\}$, $f \in \mathbb{K}\langle \mathbf{X} \rangle$
Output: g, a reduced normal form of f w.r.t. G

```
Set g = f.
while τ_i acts non-trivially on g for some i ∈ J do
    g = τ_i(g);
end while;

return g;
```

1.39 Remark. It is still not clear that the normal form is unique and in fact it is not. This is due to the fact that G is an arbitrary generating set and the construction of the normal form given in the algorithm depends on the choice of the reductor. The normal form will become unique once we find a special Gröbner basis, such that the choices we have to make are minimal.
Moreover we have no guarantee that the procedure terminates. Therefore one needs to introduce the notion of reduction-finite elements, which is in general a property induced by the ordering. For details we refer the interested reader to [Stu10]. For now we just introduce the properties which are required for a normal form in order to be unique.

1.40 Definition. Let $G \subset \mathbb{K}\langle \mathbf{X} \rangle$ and $\langle G \rangle =: I$.

- G is called *simplified* or *minimal*, if $\mathtt{lm}(g) \notin \mathtt{L}(G \setminus \{g\}) \quad \forall g \in G$.
- G is called *reduced* Gröbner basis, if G is simplified, a Gröbner basis and for every $g \in G$ we have:
  1. g is monic.
  2. $g - \mathtt{lm}(g)$ is in reduced normal form with respect to I.

1.41 Remark. Note that we build the normal form with respect to I. This is only a technical issue: in fact it would be absolutely equivalent if we had demanded a normal form with respect to G, since a Gröbner basis is a generating set and if a monomial is divisible by some leading monomial of a polynomial contained in I, then it is divisible by a leading monomial of an element of the Gröbner basis. However, with this formulation the reduction of $g - \mathtt{lm}(g)$ does not depend on the choice of the Gröbner basisas long as the ordering is fixed.
In order to prove the existence of a unique normal form one has to introduce the term of *reduction-unique* elements. We will not go into detail about that here, as stated before, but it is important that a reduced Gröbner basis allows one to compute a unique normal form with respect to a fixed monomial ordering.

1.3.1 The Gröbner basis algorithm

For this section we will always assume that our ideal I is finitely generated, due to the fact that we want to do some computations, which would be quite difficult if we start with an infinite generating set. Nevertheless this assumption is not necessary. Note that even with a finite generating set we may get a Gröbner basis which is infinite, as we will see in an example later on. We will follow mainly [Stu10].
Again we may assume that all polynomials in a generating set are monic.

1.42 Definition. Let $G = \{g_1, \ldots, g_\omega\} \subset \mathbb{K}\langle \mathbf{X} \rangle$.
We call a polynomial f *weak* with respect to G, if $f = \sum_{k=1}^{\omega} \sum_{j} c_{k,j} l_{k,j} g_k r_{k,j}$, where $c_{k,j} \in \mathbb{K}$ and $l_{k,j}, r_{k,j} \in \mathbf{X}$ such that $l_{k,j}\mathtt{lm}(g_k)r_{k,j} \leq \mathtt{lm}(f)\ \forall k = 1, \ldots, \omega$.
Let $H \subset \mathbb{K}\langle \mathbf{X} \rangle$. A polynomial f is called *reducible* from H with respect to G, if weakness with respect to G of all elements of H implies weakness of f with respect to G.

Note that weakness is a special form of generating f with elements of G. Since it is allowed to use the same generator more than one time it should be allowed for weakness as well. For example the polynomial $p := xy + yx + xyx \in \langle y \rangle$ should be weak with respect to $\{y\}$.
Again one may avoid the twin-sum in the definition of weakness by considering the enveloping algebra.

1.43 Definition. Let $G = \{g_i \mid 1 \leq i \leq \omega\}$ be a set of monic polynomials. An *obstruction* of G is a six-tuple $(l, i, r; \lambda, j, \rho)$ with $1 \leq i, j \leq \omega$ and $l, r, \lambda, \rho \in \mathbf{X}$ such that $\mathtt{lm}(g_i) \leq \mathtt{lm}(g_j)$ and $l\mathtt{lm}(g_i)r = \lambda\mathtt{lm}(g_j)\rho$. For any given obstruction we define the corresponding *S-polynomial* as $s(l, i, r; \lambda, j, \rho) = lg_ir - \lambda g_j\rho$. A set D of polynomials is called *basic* for G if every S-polynomial of G is reducible from D with respect to G.

1.44 Motivation. Starting with a generating set for I the set of all non-weak S-polynomials will be a Gröbner basis. This seems to be an easy way to compute a Gröbner basis, since one only has to compute all S-polynomials and check if they are weak or not. This procedure has the disadvantage that it would take forever, literally, since the set of all obstructions is infinite. So our medium-term issue is to discard most of these obstructions.

1.45 Lemma. Let $G = \{g_i \mid 1 \leq i \leq \omega\}$ be a set of monic polynomials and $(l, i, r; \lambda, j, \rho)$ a *weak obstruction*, that is, the corresponding S-polynomial is weak with respect to G. Then all obstructions $(\tilde{l}, i, \tilde{r}; \tilde{\lambda}, j, \tilde{\rho})$ with $\tilde{l} = w_1 l$, $\tilde{r} = rw_2$, $\tilde{\lambda} = w_1\lambda$ and $\tilde{\rho} = \rho w_2$, where w_1, w_2 are arbitrary monomials, are also weak.

Proof: Set $s := s(l, i, r; \lambda, j, \rho)$ and $\tilde{s} := s(\tilde{l}, i, \tilde{r}; \tilde{\lambda}, j, \tilde{\rho})$. Because the obstruction is weak we can write $s = lg_ir - \lambda g_j\rho = \sum_{k=1}^{\omega} \sum_{l} c_{k,l} l_{k,l} g_k r_{k,l}$ with $c_{k,l} \in \mathbb{K}$,$l_{k,l}, r_{k,l} \in \mathbf{X}$, $l_{k,l}\mathtt{lm}(g_k)r_{k,l} \leq \mathtt{lm}(s)$ $\forall k = 1, \ldots, \omega$. Now we have $\tilde{s} = \tilde{l}g_i\tilde{r} - \tilde{\lambda}g_j\tilde{\rho} = w_1(lg_ir - \lambda g_j\rho)w_2 = w_1 s w_2 = w_1(\sum_{k=1}^{\omega} \sum_{l} c_{k,l} l_{k,l} g_k r_{k,l})w_2 = \sum_{k=1}^{\omega} \sum_{l} c_{k,l} \tilde{l}_{k,l} g_k \tilde{r}_{k,l}$ with
$\tilde{l}_{k,l} = w_1 l_{k,l}$ and $\tilde{r}_{k,l} = r_{k,l} w_2$.
Furthermore we see that $\tilde{l}_{k,l}\mathtt{lm}(g_k)\tilde{r}_{k,l} \leq w_1\mathtt{lm}(s)w_2 = \mathtt{lm}(\tilde{s})$, which shows that $\tilde{s}$ is weak with respect to G. q.e.d.

So *multiples* of obstructions need not be considered. However the set we have to consider is still infinite. But the lemma helps us to prove our claim in 1.44.

1.46 Theorem. For a set G of polynomials generating an ideal I of $\mathbb{K}\langle\mathbf{X}\rangle$, the following statements are equivalent:

(i) G is a Gröbner basis.

(ii) The reduced normal form of each polynomial in I is equal to 0.

(iii) Each S-polynomial of G is weak with respect to G.

(iv) The empty set is a basic set for G.

Proof:
$(i) \Longrightarrow (ii)$: Induction with respect to the monomial ordering $<$:
The normal form of 0 equals 0. Take $0 \neq f \in I$ and assume f is monic.

Since G is a Gröbner basis there exists $g \in G$ such that $\mathtt{lm}(g) \mid \mathtt{lm}(f)$, that is, $\exists l, r \in \mathbf{X} : \ l\mathtt{lm}(g)r = \mathtt{lm}(f)$. Because of $f, g \in I$ we have $\tilde{f} := f - lgr \in I$ and $\deg(\tilde{f}) < \deg(f)$. By the induction hypothesis, the normal form of $\tilde{f}$ equals zero and we obtain that the normal form of f equals zero as well.
$(ii) \Longrightarrow (iii)$: Suppose $s = s(l, i, r; \lambda, j, \rho)$. By assumption the normal form of s with respect to G equals 0, so s is weak by the definition of weakness.
$(iii) \Longleftrightarrow (iv)$: Clear by definition.
$(iii) \Longrightarrow (i)$: Suppose $f \in I$, but $\mathtt{lm}(f) \notin \langle \{\mathtt{lm}(g) \mid g \in G\} \rangle$ and $\mathtt{lm}(f)$ is minimal with respect to $<$. Now there are at least two polynomials $g_i, g_j \in G$, $g_i \neq g_j$, such that $f = \sum_l c_{i,l} l_{i,l} g_i r_{i,l} + \sum_l c_{j,l} l_{j,l} g_j r_{j,l} + \sum_{g_k \in G, g_k \neq g_i, g_j} \sum_l c_{k,l} l_{k,l} g_k r_{k,l}$, $c_{k,l} \in \mathbb{K}$, $l_{k,l}, r_{k,l} \in \mathbf{X}$ $\forall k$ and $t := \mathtt{lm}(\sum_l l_{i,l} g_i r_{i,l}) = \mathtt{lm}(\sum_l l_{j,l} g_j r_{j,l}) > \mathtt{lm}(f)$.
Now by assumption $s := s(\mathtt{lm}(l_{i,l}), i, \mathtt{lm}(r_{i,l}); \mathtt{lm}(l_{j,l}), j, \mathtt{lm}(r_{j,l}))$ is weak and $s = \sum_{k \in \mathbb{J}} \sum_l a_{k,l} g_k b_{k,l}$, where $\mathbb{J}$ is an arbitrary set of indices and $g_k \in G$, such that all leading terms of g_k are smaller than t. Then $f = \sum_l \mathtt{lc}(l_{i,l} r_{i,l}) \mathtt{lc}(l_{j,l} r_{j,l})^{-1} l_{j,l} g_j r_{j,l} + \sum_l \mathtt{lc}(l_{i,l} r_{i,l}) \sum_{k \in \mathbb{J}} a_{k,l} g_k b_{k,l} + \sum_{h \neq i,j} \sum_l l_{h,l} g_h r_{h,l}$ is an expression of f with fewer summands with leading term equal to t. If we do this iteratively until we have only one term equal to t left, we reach a contradiction and we can conclude that G is a Gröbner basis. q.e.d.

Note that the generating set is not taken to be finite. If we do not enumerate the polynomials in a generating set G, we often write $(l, g, r; \lambda, p, \rho)$ for the obstruction of $g, p \in G$.
Now we focus on finding a finite set of obstructions, from which we can construct a Gröbner basis. Therefore we introduce the concept of overlap.

1.47 Definition. We say two monomials $t_1, t_2 \in \mathbf{X}$ have *overlap* $b \in \mathbf{X}$ or *overlap at* $b \in \boldsymbol{X}$ if there are $a, c \in \mathbf{X}$ such that $t_1 = ab$ and $t_2 = bc$ or $t_1 = ba$ and $t_2 = cb$ or $t_1 = b$ and $t_2 = abc$. If 1 is the only overlap between t_1 and t_2 we say the monomials have *no overlap*. Equivalently the monomials are called *coprime*.
An obstruction $(l, i, r; \lambda, j, \rho)$ is said to have *no overlap* if there exists $w \in \mathbf{X}$ such that $l\mathtt{lm}(g_i)r = l\mathtt{lm}(g_i)w\mathtt{lm}(g_j)\rho$ or $l\mathtt{lm}(g_i)r = \lambda\mathtt{lm}(g_j)w\mathtt{lm}(g_i)r$.

This generalizes the notion of a common divisor. As in the commutative case one wants to construct only those S-polynomials which do not reduce to zero or at least as few as possible more. Therefore the next propositions are useful.

1.48 Lemma (Product Criterion)**.** Let $g_1, g_2 \in \mathbb{K}\langle \mathbf{X} \rangle$ be such that $l_1 := \mathtt{lm}(g_1)$ and $l_2 := \mathtt{lm}(g_2)$ have no overlap. Then every obstruction $(l, g_1, r; \lambda, g_2, \rho)$ with $l, r, \lambda, \rho \in \mathbf{X}$ has no overlap.

Proof: Since l_1 and l_2 have no overlap $\mathtt{lm}(lg_1r) = \mathtt{lm}(\lambda g_2 \rho)$ implies that either ll_1 and λ or $l_1 r$ and ρ have overlap l_1.
Assume the first case is true. Then r and l_2 overlap at l_2, say $r = l_2\overline{r}$. Then

$\overline{r} = \rho$ and therefore $ll_1r = ll_1l_2\overline{r} = ll_1l_2\rho$ which shows that $(l, g_1, r; \lambda, g_2, \rho)$ has no overlap.
Now if l_1r and ρ overlap at l_1 then l and λl_2 have overlap l_2 and $l = \bar{l}l_2 = \lambda l_2$. Hence we get $ll_1r = \lambda l_2 l_1 r$ and again we obtain that $(l, g_1, r; \lambda, g_2, \rho)$ has no overlap. q.e.d.

1.49 Theorem. Let $G = \{g_i \mid i = 1, \ldots, \omega\} \subset \mathbb{K}\langle \mathbf{X}\rangle$. Every obstruction without overlap is reducible from an S-polynomial with overlap with respect to G.

Proof: Let $b = (l, i, r; \lambda, j, \rho)$ be an obstruction without overlap and denote by s its S-polynomial. Since $l\mathtt{lm}(g_i)r = \lambda\mathtt{lm}(g_j)\rho$ we have either $r = w\mathtt{lm}(g_j)\rho$ or $l = \lambda\mathtt{lm}(g_i)w$.
If the former is valid then we also have $\lambda = l\mathtt{lm}(g_i)w$ and by Lemma 1.45 $b = (l, i, w\mathtt{lm}(g_j)\rho; l\mathtt{lm}(g_i)w, j, \rho)$ is reducible from $(1, i, w\mathtt{lm}(g_j); \mathtt{lm}(g_i)w, j, 1)$. Therefore we assume $l = \rho = 1$.
Write $g_i = \sum_h c_h t_h$, $g_j = \sum_p d_p u_p$ with $t_h, u_p \in \langle \mathbf{X}\rangle$, $c_h, d_p \in \mathbb{K} \setminus \{0\}$, such that $t_h > t_{h+1}$ and $u_p > u_{p+1}$. Now $s = g_i r - \lambda g_j = g_i w\mathtt{lm}(g_j) - \mathtt{lm}(g_i)wg_j = g_i w(g_j - \sum_{p,p\neq 1} d_p u_p) - (g_i - \sum_{h,h\neq 1} c_h t_h)wg_j = \sum_{h,h\neq 1} c_h t_h w g_j - \sum_{p,p\neq 1} d_p g_i w u_p$. Assume $c_2 t_2 w u_1 = d_2 t_1 w u_2$, that is the leading terms $t_2 w\mathtt{lm}(g_j)$ and $\mathtt{lm}(g_i)wu_2$ of the two summations cancel each other. Since $t_2 < t_1$ and $u_2 < u_1$ this only occurs if $c_2 = d_2$ and there are $v_1, v_2 \in \langle \mathbf{X}\rangle$, such that $t_1 = t_2 v_1$ and $u_1 = v_2 u_2$ with $v_1 w = w v_2$. If w is a left divisor of v_1, say $v_1 = w v_1'$, then $v_2 = v_2' w$, which implies that $v_1' = v_2'$ and therefore $(1, i, w\mathtt{lm}(g_j); \mathtt{lm}(g_i)w, j, 1)$ is reducible from $(1, i, v_1'\mathtt{lm}(g_j); \mathtt{lm}(g_i)v_1', j, 1)$ by Lemma 1.45. If w is not a left divisor of v_1, then w has a self overlap, that is, $w = v_1 w' = w' v_2$. and again we apply Lemma 1.45. So we may assume $w = 1$ that is, $b = (1, i, \mathtt{lm}(g_j); \mathtt{lm}(g_i), j, 1)$. We find

$$s = g_i\mathtt{lm}(g_j) - \mathtt{lm}(g_i)g_j = lm(g_i)\mathtt{lm}(g_j) + \sum_{h,h\neq 1} c_h t_h \mathtt{lm}(g_j) - lm(g_i)\mathtt{lm}(g_j)$$
$$- \sum_{p,p\neq 1} \mathtt{lm}(g_i) d_p u_p = \sum_{h,h\neq 1} c_h t_h (g_j - \sum_{p,p\neq 1} d_p u_p) - \sum_{p,p\neq 1} (g_i - \sum_{h,h\neq 1} c_h t_h) d_p u_p$$
$$= (\sum_{h,h\neq 1} c_h t_h) g_j - g_i (\sum_{p,p\neq 1} d_p u_p) \in \langle g_i, g_j\rangle,$$

so s is weak with respect to G, which implies that it is reducible from G. q.e.d.

The theorem states: If an S-polynomial $s(l, g_i, r; \lambda, g_j, \rho)$ is not weak with respect to G, then the leading monomials of the two polynomials g_i and g_j have an overlap. This will help us to find a finite basic set.

1.50 Lemma. Let $G = \{g_i \mid i = 1, \ldots, \omega\} \subset \mathbb{K}\langle \mathbf{X}\rangle$. There is a finite basic set D of S-polynomials of G, such that every S-polynomial of G in D corresponds to an obstruction $(l, i, r; \lambda, j, \rho)$ with overlap and with either one of the two parameters $\{l, \lambda\}$ and one of $\{r, \rho\}$ equal to 1 or $\lambda = \rho = 1$.

Proof: We write $s = s(l, i, r; \lambda, j, \rho)$, $\mathtt{lm}(g_i) = m_1 \dots m_p$ and $\mathtt{lm}(g_j) = n_1 \dots n_q$ with $m_k, n_{\tilde{k}} \in \langle \mathbf{X} \rangle$ of degree 1, $k = 1, \dots, p; \tilde{k} = 1, \dots, q$ (this means that each m_k and $n_{\tilde{k}}$ corresponds to an $x_i, i = 1, \dots, n$). Now if s is not weak, then it must have some overlap. In particular, $\mathtt{lm}(g_i)$ and $\mathtt{lm}(g_j)$ must overlap. This can occur in three ways:

$$\begin{aligned} m_1 \cdots m_h &= n_{q-h+1} \cdots n_q, & 1 \leq h < p, \\ n_1 \cdots n_h &= m_{p-h+1} \cdots m_p, & 1 \leq h < p, \\ m_1 \cdots m_p &= n_{h+1} \cdots n_{h+p}, & 1 \leq h < q - p. \end{aligned}$$

In particular, for every two polynomials the number of possible overlaps is finite. We show that D needs to contain at most one S-polynomial for every overlap, which completes the proof. Assume $\mathtt{lm}(g_i)$ and $\mathtt{lm}(g_j)$ have nontrivial overlap. To satisfy the equation $l\mathtt{lm}(g_i)r = \lambda\mathtt{lm}(g_j)\rho$, the factors that are not in the overlap have to be in λ or ρ respectively in l or r (cf. proof of Lemma 1.48). So for every obstruction corresponding to some overlap the monomials $l\mathtt{lm}(g_i)r$ and $\lambda\mathtt{lm}(g_j)\rho$ have to be equal to $\tilde{l}w\tilde{r}$ and $\tilde{\lambda}w\tilde{\rho}$, respectively, with w equal to

$$\begin{aligned} w &= n_1 \cdots n_{q-h}\mathtt{lm}(g_i) && = \mathtt{lm}(g_j)m_{h+1} \cdots m_p, \\ w &= \mathtt{lm}(g_i)n_{h+1} \cdots n_q && = m_1 \cdots m_{p-h}\mathtt{lm}(g_j), \\ w &= n_1 \cdots n_h\mathtt{lm}(g_i)n_{h+p+1} \cdots n_q && = \mathtt{lm}(g_j), \end{aligned}$$

in the respective cases. Now by Lemma 1.45 these obstructions are weak except when $\tilde{l} = \tilde{r} = \tilde{\lambda} = \tilde{\rho} = 1$. So for every possible overlap there exists a single S-polynomial such that all other obstructions are reducible from it with respect to $\{g_i, g_j\}$. In the respective cases, the corresponding obstructions are

$$\begin{gathered} (n_1 \cdots n_{q-h}, i, 1; 1, j, m_{h+1} \cdots m_p), \\ (1, i, n_{h+1} \cdots n_q; m_1 \cdots m_{p-h}, j, 1), \\ (n_1 \cdots n_h, i, n_{h+p+1} \cdots n_q; 1, j, 1). \end{gathered}$$

This means that s need only to be in D if at least one of the two parameters l and λ and one of the two parameters r and ρ are equal to 1. q.e.d.

We refer to the S-polynomial corresponding to an overlap $\omega = (l, g, r; \lambda, g', \rho)$, we have to consider, as $S(\omega)$.

We distinguish between three kinds of obstructions:

1.51 Definition. Let $s = (l, i, r; \lambda, j, \rho)$ be an obstruction of the set $G = \{g_i \mid 1 \leq i \leq \omega\}$ of monic polynomials in $\mathbb{K}\langle \mathbf{X} \rangle$.

- If $l = 1$, then we call s a *right obstruction.*
- If $l \neq 1$ and $r = 1$, then we call s a *left obstruction.*

- If s is not a right nor a left obstruction and $\lambda = \rho = 1$, then we call s a *central obstruction*.

1.52 Corollary. Let G be a set of polynomials in $\mathbb{K}\langle \mathbf{X} \rangle$ and let D be the set of all non-zero normal forms of S-polynomials with respect to G corresponding to all left, right and central obstructions of G. Then D is a basic set for G.

In the definition above the restriction to a finite set G is not necessary, since an obstruction includes only two polynomials. However, as stated before, for "real-life" computations finiteness is required and so we will assume for the rest of this section that $G = \{g_i \mid 1 \leq i \leq \omega\}$.

We finally introduce an algorithm that computes a reduced Gröbner basis.

1.53 Definition. Let I be a two-sided ideal of $\mathbb{K}\langle \mathbf{X} \rangle$ and let G, D be subsets of $\mathbb{K}\langle \mathbf{X} \rangle$. We say that (G, D) is a *partial Gröbner pair* for I if the following properties are satisfied:

1. All polynomials in $G \cup D$ are monic.
2. G is a generating set of I.
3. Every element of D belongs to I and it is in normal form with respect to the polynomials in G.
4. The set D is basic for G.
5. For every $f \in G$ the normal form with respect to $G \cup D$ of the normal form with respect to $G \setminus \{f\}$ equals zero.

1.54 Remark. Let I be a two-sided ideal in $\mathbb{K}\langle \mathbf{X} \rangle$ and let (G, D) be a partial Gröbner pair for I. If D is the empty set, then G is a Gröbner basis.

Since $\mathbb{K}\langle \mathbf{X} \rangle$ is not Noetherian, for example the ideal $\langle x_1 x_2^n x_1 \mid n \in \mathbb{N} \rangle$ can not be finitely generated, our algorithm may not terminate in all cases. However, we will see later that we can use this algorithm to get some important results after finitely many steps.

1.55 Algorithm.

Input: a (finite) generating set G for $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$

Output: a reduced Gröbner basis for I

Compute all non-zero normal forms of S-polynomials with respect to G corresponding to all left, right and central obstructions of G and call the resulting set D. Then (G, D) is a partial Gröbner pair. Construct a new partial Gröbner pair $(\tilde{G}, \tilde{D})$ as follows:

1. Take $f \in D$ and set $\tilde{G} = \{g_1, \ldots, g_\omega, g_{\omega+1} := f\}$.

2. Compute the left, right and central obstructions of $\tilde{G}$ of the form $(l, i, r; \lambda, \omega+1, \rho)$ and $(l, \omega+1, r; \lambda, j, \rho)$ for certain $i, j \in \{1, \ldots, \omega\}$ and $l, r, \lambda, \rho \in \langle \mathbf{X} \rangle$ and put the non-zero normal forms of their S-polynomials with respect to $G \cup D$ in D, such that D becomes a basic set for $\tilde{G}$. Call this new basic set $\tilde{D}$.

3. For each $i \in \{1, \ldots, \omega\}$ compute the normal form g_i' with respect to $\tilde{G} \setminus \{g_i\}$ of g_i. If $g_i' = 0$ remove g_i from $\tilde{G}$. Otherwise, if g_i' is distinct from g_i,
   a) replace g_i by g_i';
   b) compute the left, right and central obstructions of the new $\tilde{G}$ involving g_i';
   c) if the normal form with respect to $\tilde{G} \cup \tilde{D}$ of an S-polynomial of such an obstruction is non-zero then add its normal form to $\tilde{D}$.

4. Replace each $d \in \tilde{D}$ by its normal form with respect to $(\tilde{G} \cup \tilde{D}) \setminus \{d\}$.

1.56 Theorem. In the situation of 1.55, the ideal generated by the leading monomials of G is strictly contained in the ideal generated by the leading monomials of $\tilde{G}$. If $\tilde{D} = \emptyset$ then $\tilde{G}$ is a Gröbner basis for I (and the routine stops).

Proof: First we have to show that $(\tilde{G}, \tilde{D})$ is a partial Gröbner pair, which means we have to verify condition one to five of Definition 1.53.
Since all polynomials in $\tilde{G}$ and $\tilde{D}$ are normal forms, they are monic, we get condition 1.
If $g_i \in \tilde{G}$ adjusted as in step 4 of the algorithm, then the ideal generated by $\{g_i'\} \cup (G \setminus \{g_i\})$ coincides with I, so we get condition 2.
Clearly all elements of $\tilde{D}$ belong to I and are in normal form with respect to $\tilde{G}$ and this is condition 3.
Because of 1.52, $\tilde{D}$ is a basic set for G and hence condition 4.
For every element $g \in \tilde{G} \setminus G$, the normal forms of the newly computed central obstructions of G involving g take care of condition 5.
That $\mathtt{L}(G) \subset \mathtt{L}(\tilde{G})$ is valid follows immediately from the construction we have made.
The final assertion is a consequence of Remark 1.54. q.e.d.

1.57 Example. For all examples we take the lexicographical ordering with $x_1 > x_2 > \ldots > x_n$ or $x > y > z$ respectively.

- Take $\mathbb{K}\langle x, y \rangle$ and $G_1 = \{xyx + y^2\}$.
  There is only one obstruction to consider, since the only central obstruction are the trivial ones and every left obstruction is equal to a right obstruction, namely $(xy, 1, 1; 1, 1, yx) = xy^3 - y^3x$. $\Longrightarrow D_1 = \{xy^3 - y^3x\}$.
  Now $G_2 = \{xyx + y^2, xy^3 - y^3x\}$, since $xy^3 - y^3x$ is in normal form with

respect to g_1.
Because our new g_2 only has trivial obstruction with itself, there is only one new obstruction: $(1,1,y^3;xy,2,1) = y^5 + xy^4x$, which has normal form 0 with respect to G_2, so G_2 is a Gröbner basis for $I = \langle G_1 \rangle$.

- Take $G = \{x_ix_j - x_jx_i \mid 1 \leq i < j \leq n\} \subset \mathbb{K}\langle \mathbf{X} \rangle$. We claim that G is already a Gröbner basis.
The only non-trivial overlaps are given by the polynomials $x_ix_j - x_jx_i$ and $x_jx_w - x_wx_j$, where $1 \leq i < j < w \leq n$. The S-polynomial can be computed by $(x_ix_j - x_jx_i)x_w - x_i(x_jx_w - x_wx_j) = x_ix_wx_j - x_jx_ix_w$ which reduces to zero, using the leading monomials of $x_ix_w - x_wx_i,\ x_jx_w - x_wx_j$ and $x_ix_j - x_jx_i \in G$.
Note that G generates the *commutator ideal*, so we have $\mathbb{K}[x_1, \ldots, n] \cong \mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle$.

- Let us consider the generating set $B = \{yzxy - xyzx, zxyz - xyzx, zxyz - yzxy\} \subseteq \mathbb{K}\langle x,y,z \rangle$, which consists of *braid relations* (cf. [Gar07]). Then the unique reduced Gröbner basis is given by $G = \{yzxy - zxyz, xyzx - zxyz, xzxyz - zxyzy, yz^nxyz - zxyz^2x^{n-1}, xz^nxyz - zxyzyx^{n-1} \mid n \in \mathbb{N}\}$.
Obviously, none of the elements of G is redundant.
To see that G is in fact a Gröbner basis one has to consider all pairs (g_i, g_j) of elements of G and check if all possible obstructions of (g_i, g_j) vanish to zero. We demonstrate this for $w_1 := yz^nxyz - zxyz^2x^{n-1}$ and $w_2 := yz^mxyz - zxyz^2x^{m-1}$ for arbitrary $n, m \in \mathbb{N}$. We only have to worry about the right overlap, since n and m are arbitrary elements in $\mathbb{N}$ (so we can exchange their places for the left overlap). Now w_1 and w_2 overlap at yz and we have:

$$
\begin{aligned}
&(yz^nxyz - zxyz^2x^{n-1}) \cdot z^{m-1}xyz - yz^nx \cdot (yz^mxyz - zxyz^2x^{m-1}) \\
&= && - zxyz^2x^{n-1}z^{m-1}xyz + yz^nxzxyz^2x^{m-1} \\
&\xrightarrow{xzxyz - zxyzy} && yz^{n+1}xyzyzx^{m-1} - zxyz^2x^{n-1}z^{m-1}xyz \\
&\xrightarrow{yz^{n+1}xyz - zxyz^2x^n} && zxyz^2x^nyzx^{m-1} - zxyz^2x^{n-1}z^{m-1}xyz \\
&\xrightarrow{xyzx - zxyz} && zxyz^2x^{n-1}zxyzx^{m-2} - zxyz^2x^{n-1}z^{m-1}xyz \\
&\xrightarrow{xyzx - zxyz} && zxyz^2x^{n-1}z^2xyzx^{m-3} - zxyz^2x^{n-1}z^{m-1}xyz \\
&\xrightarrow{xz^2xyz - zxyzyx} && zxyz^2x^{n-2}zxyzyx^{m-2} - zxyz^2x^{n-1}z^{m-1}xyz \\
&\xrightarrow{xzxyz - zxyzy} && zxyz^2x^{n-3}zxyzy^2x^{m-2} - zxyz^2x^{n-1}z^{m-1}xyz \\
&\xrightarrow{xz^{m-1}xyz - zxyzyx^{m-2}} && zxyz^2x^{n-3}zxyzy^2x^{m-2} - zxyz^2x^{n-2}zxyzyx^{m-2} \\
&\xrightarrow{xzxyz - zxyzy} && 0.
\end{aligned}
$$

This example also shows that a Gröbner basis does not need to be finite, even if the ideal is finitely generated.

1.3.2 Improvement to the algorithm

In commutative as well as non-commutative Gröbner basis theory it is well-known, that the practical use of criteria to reduce the set of critical pairs has very effective impact on the performance. Out of several criteria, first formulated by Buchberger, the product criterion in the case of free algebras is naturally appearing during the consideration of overlaps of polynomials. The chain criterion applies, but it can be refined further, following the work of Gebauer and Möller [GM88] in the commutative case.

Gebauer-Möller's criterion has been generalized to the setup of modules in [KR00] and [KR05], while in the non-commutative case Mora gave a detailed presentation of superfluous pairs in [Mor94], which was adapted to fit practical computations, as for example in [Xiu12].
Here we will presented the theoretical layout and then study the practical use of the criterion in a later chapter.

For this section we will assume that each set $P \subset \mathbb{K}\langle \mathbf{X} \rangle$ is *interreduced*, meaning $\forall p, q \in P, p \neq q : \mathtt{lm}(p) \nmid \mathtt{lm}(q)$ and that each $p \in P$ is monic.

Recall that the Product Criterion Theorem 1.48 states that only those pairs involving an overlap need to be considered, that is $\mathtt{lm}(p) = ab$ and $\mathtt{lm}(q) = bc$ for some monomials a, b, c. Therefore one only has to consider pairs $\pi = (1, p_i, r; \lambda, p_j, 1)$, such that $\mathtt{lm}(p_i r) = \mathtt{lm}(\lambda p_j)$.

1.58 Definition. For an obstruction $\pi = (1, p_i, r; \lambda, p_j, 1)$ we denote by $\mathtt{cm}(\pi) := \mathtt{lm}(p_i r) = \mathtt{lm}(p_i) r = \lambda \mathtt{lm}(p_j)$ the common multiple of p_i and p_j with respect to the overlap considered in π.

Let us consider a set of polynomials P and construct the set of all critical pairs $\pi(P)$ by searching for overlaps in the leading monomials, that is $\pi(P)$ contains all those elements we want to compute S-polynomials to enter the set D in the algorithm. We want to apply the criteria to $\pi(P)$ to reduce its size.

1.59 Theorem. Assume we have a set of polynomials P, its set of critical pairs $\pi(P)$ and a pair $\pi = (1, p_i, r_i; \lambda_k, p_k, 1) \in \pi(P)$.

1. If there exist two pairs $\pi_1 = (1, p_i, r_i'; \lambda_j, p_j, 1), \pi_2 = (1, p_j, r_j; \lambda_k', p_k, 1) \in \pi(P) \setminus \{\pi\}$, such that $\mathtt{lm}(p_j) | \mathtt{cm}(\pi)$, then the S-polynomial $s(\pi)$ of π will reduce to zero.

2. If there exists a pair $\pi_1 = (1, p_j, r_j; \lambda_k', p_k, 1) \in \pi(P) \setminus \{\pi\}$, such that $\mathtt{cm}(\pi_1)$ divides $\mathtt{cm}(\pi)$ from the right, then the S-polynomial $s(\pi)$ of π will reduce to zero.

Proof:

1. Because of the assumptions we have $\mathtt{lm}(f_j) = abc$, $\mathtt{lm}(f_k) = bct_k$ and $\mathtt{lm}(f_i) = t_iab$ for some monomials a, b, c, t_i, t_k. Since P is interreduced, none of the leading monomials can divide the overlap cofactors. This implies $\lambda_k = t_ia$ and $r_i = ct_k$. Moreover, the existence of π_1 and π_2 and the form of the leading monomials imply that there exist pairs $\pi_1' = (1, p_i, c; t_i, p_j, 1)$ and $\pi_2' = (1, p_j, t_k; a, p_k, 1)$. Then

$$\begin{aligned} s(\pi) &= p_ict_k - t_iap_k = t_iabct_k + \mathtt{tail}(p_i)ct_k - t_iabct_k - t_ia\mathtt{tail}(p_k) \\ &\to -t_i\mathtt{tail}(p_j)t_k + \mathtt{tail}(p_i)ct_k + t_i\mathtt{tail}(p_j)t_k - t_ia\mathtt{tail}(p_k) \\ &= -s(\pi_1')t_k - t_is(\pi_s') \to 0. \end{aligned}$$

   Note that the reductions used are performed according to the fixed monomial ordering.

2. We first note that $\mathtt{lm}(p_j)r_j = \mathtt{lm}(p_jr_j) = \mathtt{lm}(\lambda_k'p_k) = \lambda_k'\mathtt{lm}(p_k)$ and $\tilde{l}\mathtt{lm}(p_j)r_j = \tilde{\lambda}\lambda_k'\mathtt{lm}(p_k) = \lambda_k\mathtt{lm}(p_k) = \mathtt{lm}(p_i)r_i$ for some monomials $\tilde{l}, \tilde{\lambda}$. This already implies $\tilde{l} = \tilde{\lambda}$ and $\tilde{\lambda}\lambda' = \lambda_k$. Moreover, $\tilde{l}\mathtt{lm}(p_j)r_j = \mathtt{lm}(p_i)r_i$ implies that one of the following holds:
   - $\tilde{l}\mathtt{lm}(p_j)|\mathtt{lm}(p_i)$. Then the set of polynomials is not interreduced, which leads to a contradiction.
   - There exists $\hat{r}_i$ such that $r_j = \hat{r}_ir_i$. This implies the existence of a pair $(1, p_i, \hat{r}_i; \tilde{l}, p_j, 1)$ and the claim follows from the first case. q.e.d.

1.60 Remark. One can apply these criteria in a straightforward way: If the set of critical pairs during some step of Buchberger's algorithm has been constructed, then one can just check the pairs and search for redundant ones. However, to decide if a monomial divides another is not as cheap and easy as in the commutative case.

In the next chapter we will study a new approach to Gröbner basis theory and will later on investigate the possibilities this holds to apply the criteria.

1.4 Conclusion

While the aim of this chapter is to introduce Gröbner basis theory over the free algebra and there are several works which have similar chapters (for example [Li12] and [Stu10]) the translation of the Gebauer-Möller criteria is rather new. We like to point out that this was also studied in [Xiu12] and later published in [KX13] and that this work was developed in parallel to our approach. The results presented for the implementation in ApCocoa show, similarly to ours, that those criteria are indeed speeding up the computations by quite a lot.

As mentioned before there is a deficit in proper studies of orderings over the free algebra. While we are not able to give a full classification in the frame of this work we hope to motivate further studies with this first approach to present more than one useful ordering.

Since orderings have a huge impact on the complexity of computations it is necessary to get a good insight into the topic. In the next chapter we will discuss how orderings for the free algebra can be represented over the letterplace ring. This is done to understand the properties of orderings.

2 The Letterplace Ring

In this chapter we present the letterplace correspondence as it was studied in [LL09] and [SL13] and give a detailed overview on how to present orderings for the free algebra over the letterplace ring. We then introduce the new approach to non-graded ideals presented by Roberto La Scala in [Sca12] and show how this can be used for a new way to compute Gröbner bases using the letterplace paradigm. The structure of the letterplace ring can be exploited in a very natural way to get an efficient way to avoid the classical homogenization.

2.1 Letterplace Correspondence for graded Ideals

It is a well known fact that there exists a one to one correspondence between all ideals $J \trianglelefteq \mathbb{K}[\mathbf{X}]$ and certain ideals $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$. The question, if there is an ideal J in some commutative ring $\mathbb{K}[\mathbf{Y}]$ for each $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$, such that one can construct a one to one correspondence between those ideals and especially their Gröbner bases was studied by Roberto La Scala and Viktor Levandovskyy and led to the introduction of the *letterplace ring* (cf. [LL09]), which provides a commutative analogon of the free algebra. The basic idea, going back to Richard Feynman and Gian-Carlo Rota, is pleasingly simple: one enumerates the variables occurring in a monomial by their position in the monomial. Then one may commute the variables. In this section we will introduce this corresponding, following mainly [LL09] and [Stu10]. We start with the basic definition.

2.1 Definition. We call $\mathbf{X}$ and $P \subseteq \mathbb{N}$ respectively the *set of letters and places*. We write for the elements of the product set $\mathbf{X} \times P$: $x_i(j) := (x_i, j)$. Furthermore we denote by $\mathbb{K}[\mathbf{X} \mid P]$ the polynomial ring in the commuting variables $x_i(j)$ and by $[\mathbf{X} \mid P]$ the set of all monomials in $\mathbb{K}[\mathbf{X} \mid P]$.
Let $\mu = (\mu_k)_{k\in\mathbb{N}}, \nu = (\nu_k)_{k\in\mathbb{N}}$ be two sequences of non-negative integers with finite support. We can consider (μ, ν) as a multi-degree for the monomials $m = x_{i_1}(j_1)\dots x_{i_r}(j_r) \in [\mathbf{X} \mid P]$. Precisely, we define $\mu_k = \#\{\alpha \mid x_{i_\alpha} = x_k\}$, $\nu_k = \#\{\beta \mid j_\beta = k\}$.

Often one chooses $P = \mathbb{N}$ for theoretical questions and switches to $P = \underline{d}, \quad d \in \mathbb{N}$ for practical computations and we will see later why.

2.2 Remark. If we define $\mathbb{K}[\mathbf{X} \mid P]_{\mu,\nu}$ to be the homogeneous component of degree (μ, ν) we have $\mathbb{K}[\mathbf{X} \mid P] = \bigoplus_{\mu,\nu} \mathbb{K}[\mathbf{X} \mid P]_{\mu,\nu}$, so $\mathbb{K}[\mathbf{X} \mid P]$ is a multigraded

algebra. By putting $\mathbb{K}[\mathbf{X} \mid P]_{*,\nu} = \bigoplus_{\mu} \mathbb{K}[\mathbf{X} \mid P]_{\mu,\nu}$ and $\mathbb{K}[\mathbf{X} \mid P]_{\mu,*} = \bigoplus_{\nu} \mathbb{K}[\mathbf{X} \mid P]_{\mu,\nu}$ we obtain that $\mathbb{K}[\mathbf{X} \mid P]$ is also multigraded with respect to letter or place multidegrees only.

2.3 Example. We just want to see a simple example to visualize the letterplace analogon. So take $xyx \in \mathbb{K}\langle x, y\rangle$. Now introducing places we see that xyx corresponds to $x(0)y(1)x(2) = x(2)x(0)y(1) = y(1)x(2)x(0)$.

Unfortunately, there are some elements we have no use for, because they do not correspond to any monomial in $\mathbb{K}\langle x, y\rangle$, for example $x(3)y(6)y(9)$ and $x(0)y(0)$. So in order to get rid of those elements we want to find a subset of $\mathbb{K}[\mathbf{X} \mid P]$ that corresponds to the free algebra. Therefor we introduce the monoid action of $\mathbb{N}$.

2.4 Remark. The monoid $\mathbb{N}$ has a natural faithful action on the graded algebra $\mathbb{K}[\mathbf{X} \mid P]$ given by $s \cdot x_i(j) = x_i(j+s) \ \ \forall s \in \mathbb{N}$.

2.5 Definition. For each monomial $m = x_{i_1}(j_1) \cdots x_{i_r}(j_r) \ \in [\mathbf{X} \mid P]$ we define by $\texttt{shift}(m) = \min\{j_1, \ldots, j_r\}$ the *shift of* m.
Denote by $\mathbb{K}[\mathbf{X} \mid P]^{(s)}$ the subspace of $\mathbb{K}[\mathbf{X} \mid P]$ generated by all monomials with shift s.
For each $s, r \in \mathbb{N}$ we denote by $s \cdot 1^r$ the place-multi-degree $\nu = (\nu_k)_{k\in\mathbb{N}}$ such that

$$\nu_k = \begin{cases} 1, & \text{if } s \leq k \leq s + r - 1. \\ 0, & \text{otherwise.} \end{cases}$$

For $s = 0$ we write simply 1^r.
Define $V = \bigoplus_{n\in\mathbb{N}} \mathbb{K}[\mathbf{X} \mid P]_{*,1^r}$, which is a subspace of $\mathbb{K}[\mathbf{X} \mid P]^{(0)}$ and set $V' = \bigcup_{s\in\mathbb{N}} s \cdot V$.

2.6 Lemma. $\iota : \mathbb{K}\langle\mathbf{X}\rangle \to V : \ x_{i_1} \cdots x_{i_r} \mapsto x_{i_1}(0) \cdots x_{i_r}(r-1)$ is an isomorphism of vector spaces, which preserves letter-multidegrees and hence total degrees of monomials.

Proof: By the definition of ι it is obvious that ι is a $\mathbb{K}$-linear injective map. Moreover, we have $\iota^{-1} : V \to \mathbb{K}\langle\mathbf{X}\rangle : \ x_{i_1}(0) \cdots x_{i_r}(r-1) \mapsto x_{i_1} \cdots x_{i_r}$ and hence ι is bijective. Since ι is $\mathbb{K}$-linear we only have to show that ι preserves letter-multidegrees of monomials, which is clear by definition of ι. q.e.d.

So we have a vector space correspondence. However, V itself is not a ring. However, since we have identified the free algebra, it is natural to ask what happens to ideals under this correspondence.

2.7 Definition. Let J be an ideal of $\mathbb{K}[\mathbf{X} \mid P]$. Then J is called

- *place-multigraded*, if $J = \sum_{\nu} J_{*,\nu}$, where $J_{*,\nu} = J \cap \mathbb{K}[\mathbf{X} \mid P]_{*,\nu}$.

- *shift-decomposable*, if $J = \sum_s J^{(s)}$, where $J^{(s)} = J \cap \mathbb{K}[\mathbf{X} \mid P]^{(s)}$.

Clearly a place-multigraded ideal is also graded and shift-decomposable.

2.8 Lemma. Let $J \subset \mathbb{K}[\mathbf{X} \mid P]$ be an ideal. Then J is shift-decomposable if and only if J is generated by $\bigcup_{s\in\mathbb{N}} J^{(s)}$.

Proof: The necessary condition is obvious.
Assume now that $J = \langle\{mf \mid m \in [\mathbf{X} \mid P], f \in J^{(s)}, s \in \mathbb{N}\}\rangle$. Then, for $t = \min\{\mathtt{shift}(m), s\}$ we have $mf \in J^{(t)}$ and hence $J = \sum_s J^{(s)}$. q.e.d.

2.9 Definition. Let J be a shift-decomposable ideal of $\mathbb{K}[\mathbf{X} \mid P]$. We say that J is *shift-invariant* if $s \cdot J^{(t)} = J^{(s+t)}$ for all $s, t \in \mathbb{N}$.

2.10 Remark. An ideal $J \trianglelefteq \mathbb{K}[\mathbf{X} \mid P]$ is shift-invariant if and only if $s \cdot J^{(0)} = J^{(s)} \quad \forall s \in \mathbb{N}$.

2.11 Lemma. Let $J \subset \mathbb{K}[\mathbf{X} \mid P]$ be an ideal. Then J is shift-invariant if and only if $J = \sum_{s\in\mathbb{N}} s \cdot J^{(0)}$.

Proof: Clearly we have the necessary condition. Assume now $J = \sum_s s \cdot J^{(0)}$.
We have $s \cdot J^{(0)} \subset J$ and $s \cdot J^{(0)} \subset s \cdot \mathbb{K}[\mathbf{X} \mid P]^{(0)} = \mathbb{K}[\mathbf{X} \mid P]^{(s)}$ and hence $s \cdot J^{(0)} \subset J^{(s)}$. Let $f \in J^{(s)}$. Since $J = \sum_{t\in\mathbb{N}} t \cdot J^{(0)}$ we have necessarily $f \in s \cdot J^{(0)}$.
We conclude that $s \cdot J^{(0)} = J^{(s)}$ and therefore $J = \sum_{s\in\mathbb{N}} J^{(s)}$. q.e.d.

2.12 Theorem. Let J be an ideal of $\mathbb{K}[\mathbf{X} \mid P]$ an put $I = \iota^{-1}(J \cap V) \subset \mathbb{K}\langle\mathbf{X}\rangle$.

- If J is a shift-invariant ideal, then I is a left ideal of $\mathbb{K}\langle\mathbf{X}\rangle$.
- If J is a place-multigraded ideal, then I is a graded right ideal.

Proof: Assume J is shift-invariant and let $f \in I, w \in \langle\mathbf{X}\rangle$. Denote $g = \iota(f) \in J \cap V$ and $m = \iota(w)$. If $\mathrm{tdeg}(w) = s$, we have $\iota(wf) = m(s \cdot g) \in J \cap V$ and therefore $wf \in I$.
Suppose now that J is place-multigraded and hence graded. Since V is a graded subspace, it follows that $J \cap V = \sum_d (J_d \cap V)$ and then, setting $I_d = \iota^{-1}(J_d \cap V)$ we obtain $I = \sum_d I_d$. Let $f \in I_d$, that is $\iota(f) = g \in J_d \cap V$. For all $w \in \langle\mathbf{X}\rangle$ we have that $\iota(fw) = g(d \cdot m) \in J \cap V$, that is $fw \in I$. q.e.d.

2.13 Theorem. Let I be a left ideal of $\mathbb{K}\langle\mathbf{X}\rangle$ and put $I' = \iota(I)$. Define $J = \langle \bigcup_{s\in\mathbb{N}} s \cdot I'\rangle \subset \mathbb{K}[\mathbf{X} \mid P]$. Then J is a shift-invariant ideal. Moreover, if I is graded then J is place-multigraded.

Proof: From $s \cdot I' \subset J^{(s)}$ it follows that J is generated by $\bigcup_{s\in\mathbb{N}} J^{(s)}$, that is J is shift-decomposable.
By definition one has $J = \langle\{m(t\cdot f) \mid m \in [\mathbf{X} \mid P], t \in \mathbb{N}, f \in I'\}\rangle$. Then the vector space $J^{(s)}$ is spanned by the elements $m(t\cdot f)$ such that $\min\{\mathtt{shift}(m), t\} = s$. In particular, $J^{(0)}$ is spanned by the elements $m(t\cdot f)$ where $\min\{\mathtt{shift}(m), t\} = 0$. By acting with s, we obtain that $s \cdot J^{(0)}$ is spanned by elements of the form $s \cdot (m(t \cdot f)) = (s \cdot m)((s + t) \cdot f)$, where $m \in [\mathbf{X} \mid P], t \in \mathbb{N}, f \in I'$, such that $\min\{\mathtt{shift}(m), t\} = 0$ and therefore $\min\{\mathtt{shift}(s \cdot m), s + t\} = s$. Since $s \cdot \mathbb{K}[\mathbf{X} \mid P]^{(0)} = \mathbb{K}[\mathbf{X} \mid P]^{(s)}$ we conclude that $s \cdot J^{(0)} = J^{(s)}$.
Assume now that I is a graded ideal. Any element $f \in I$ can be written as $f = \sum_d f_d$, where $f_d \in I \cap \mathbb{K}\langle\mathbf{X}\rangle_d$. Put $g = \iota(f_d)$ and $g_d = \iota(f_d)$. Then $g_d \in I' \cap V_d$. For any $s \in \mathbb{N}$ one has that $s \cdot g = \sum_d s \cdot g_d$, where $s \cdot g_d \in s \cdot (I' \cap V_d) \subset J$. Note that all polynomials $s \cdot g_d$ are homogeneous with respect to place-multigrading. We conclude that J is generated by homogeneous elements and hence it is a place-multigraded ideal. q.e.d.

2.14 Definition.

- Let $I \subset \mathbb{K}\langle\mathbf{X}\rangle$ be a graded two-sided ideal. We denote by $\tilde{\iota}(I)$ the shift-invariant place-multigraded ideal $J \subset \mathbb{K}[\mathbf{X} \mid P]$ generated by $\bigcup_{s\in\mathbb{N}} s \cdot \iota(I)$, and call J the *letterplace analogon of the ideal* I.
- For a shift-invariant place-multigraded ideal $J \subset \mathbb{K}[\mathbf{X} \mid P]$ we denote by $\tilde{\iota}^{-1}(J)$ the graded two-sided ideal $I = \iota^{-1}(J \cap V) \subset \mathbb{K}\langle\mathbf{X}\rangle$.
- A graded ideal $J \subset \mathbb{K}[\mathbf{X} \mid P]$ is called a *letterplace ideal* if J is generated by $\bigcup_{s,d\in\mathbb{N}} s \cdot (J_d \cap V)$. In this case, J is shift-invariant and place-multigraded.

2.15 Remark. The map $\iota : \mathbb{K}\langle\mathbf{X}\rangle \to V$ induces a one-to-one correspondence $\tilde{\iota}$ between graded two-sided ideals I of the free associative algebra $\mathbb{K}\langle\mathbf{X}\rangle$ and the letterplace ideals J of the polynomial ring $\mathbb{K}[\mathbf{X} \mid P]$.

So now we have finally found the correspondence for an ideal in $\mathbb{K}\langle\mathbf{X}\rangle$. We are now interested in generating sets and especially Gröbner bases. If we find a correspondence we may find a Gröbner basis for a given ideal as follows: Starting with a generating set for $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ we switch to the corresponding "letterplace generating set", compute a "letterplace Gröbner basis" with commutative methods and use then the correspondence again to get our desired Gröbner basis. In this work we will only see the correspondence and acknowledge that the letterplace ring is a polynomial ring, so that commutative Gröbner theory may be applied to it.

2.16 Definition. Let J be a letterplace ideal of $\mathbb{K}[\mathbf{X} \mid P]$ and $H \subset \mathbb{K}[\mathbf{X} \mid P]$. We say that H is a *letterplace basis* of J if $H \subset \bigcup_{d\in\mathbb{N}} J_d \cap V$ and $\bigcup_{s\in\mathbb{N}} s \cdot H$ is a generating set of the ideal J.

2.17 Theorem. Let I be a graded two-sided ideal of $\mathbb{K}\langle\mathbf{X}\rangle$ and put $J = \tilde{\iota}(I)$. Moreover, let $G \subset \bigcup_{d\in\mathbb{N}} I_d$ and define $H = \iota(G) \subset \bigcup_{d\in\mathbb{N}} J_d \cap V$. Then G is a generating set of I as a two-sided ideal if and only if H is a letterplace basis of J.

Proof: Assume $\bigcup_{s\in\mathbb{N}} s \cdot H$ is a basis of J, that is, $J = \langle m(s \cdot h) \mid m \in [\mathbf{X} \mid P], s \in \mathbb{N}, h \in H\rangle$. Since J is place-multigraded, one has that $J \cap V = \langle m(s \cdot h) \in V \mid m \in [\mathbf{X} \mid P], s \in \mathbb{N}, h \in H\rangle$. If $d = \mathrm{tdeg}(h)$ then $m(s \cdot h) = m_1(s \cdot h)((s+d) \cdot m_2)$, where $m_1, m_2 \in [\mathbf{X} \mid P] \cap V$. By applying ι^{-1} we obtain that $I = \langle w_1 g w_2 \mid w_1, w_2 \in \langle\mathbf{X}\rangle, g \in G\rangle$, that is G is a generating set of I as a two-sided ideal.
Assume now G generates I. By reversing the above argument, one has that $J \cap V \subset U := \langle m(s \cdot h) \mid m \in [\mathbf{X} \mid P], s \in \mathbb{N}, h \in H\rangle \subset J$. From $s \cdot (m(t \cdot h)) = (s \cdot m)((s + t) \cdot h)\ \forall s, t \in \mathbb{N}$, it follows that $s \cdot (J \cap V) \subset U$ for any s. We conclude that $J = U$, because J is generated by $\bigcup_{s\in\mathbb{N}} s \cdot (J \cap V)$. This implies the claim. q.e.d.

So we obtain the correspondence for generating sets. For Gröbner bases however, we have to do a little more work.

2.18 Definition. Let J be an ideal of $\mathbb{K}[\mathbf{X} \mid P]$ and $H \subset J$. Then H is called a (Gröbner) *shift-basis of* J if $\bigcup_{s\in\mathbb{N}} s \cdot H$ is a (Gröbner) basis of J.

2.19 Remark.

1. If J has a shift-basis, then $s \cdot J \subset J\ \forall s \in \mathbb{N}$, that is J is shift-invariant.
2. If J is a letterplace ideal, then any letterplace basis of J is a shift-basis, but not generally a Gröbner shift-basis.
3. Let $J \subset \mathbb{K}[\mathbf{X} \mid P]$ be an ideal and $H \subset J$. Then H is a Gröbner shift-basis of J if and only if $\mathtt{lm}(H)$ is a shift-basis of $\mathtt{L}(J)$.

2.20 Lemma. Let $J \subset \mathbb{K}[\mathbf{X} \mid P]$ be a shift-invariant ideal. Then $J^{(0)}$ is a Gröbner shift-basis of the ideal J.

Proof: Clearly $J^{(0)}$ is a shift-basis of J. Let $f \in J^{(u)} \setminus \{0\}, g \in J^{(v)} \setminus \{0\}, f \neq g$ and denote the S-polynomial $s(f, g,) = cmf - dng$, where $c, d \in \mathbb{K}$ and $m, n \in [\mathbf{X} \mid P]$, such that $lcm(\mathtt{lm}(f), \mathtt{lm}(g)) = m\mathtt{lm}(f) = n\mathtt{lm}(g)$. We have to show that $s(f, g) \in \bigcup_s J^{(s)}$. If $u = v$ this is trivial. Assume $u < v$. The variables of m come from the leading monomial of g which has shift v. Therefore cmf has shift u and no variable of the leading term of g has shift u. Then the same clearly holds also for dng and therefore for $s(f, g) = cmf - dng$. q.e.d.

2.21 Remark. Before we can state the main theorem, we need a little clue: We assume our given ordering is *compatible* with ι, that is, if we fix the orderings $<$ on $\mathbb{K}\langle\mathbf{X}\rangle$ and $\prec$ on $\mathbb{K}[\mathbf{X} \mid P]$ then $v < w$ holds if and only if $\iota(v) \prec \iota(w)$ for any $v, w \in \langle\mathbf{X}\rangle$. This is no restriction, since most choices of orderings are compatible with ι.

2.22 Theorem. Let $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ be a graded two-sided ideal and put $J = \tilde{\iota}(I)$. Moreover, let H be a Gröbner letterplace basis of J and put $G = \iota^{-1}(H \cap V) \subset \bigcup_{d\in\mathbb{N}} I_d$. Then G is a Gröbner basis of I as a two-sided ideal.

Proof: Let $f \in I_d$ and put $f' = \iota(f)$. Then there is $m \in [\mathbf{X} \mid P]$, $s \in \mathbb{N}$, $h \in H$ such that $\mathtt{lm}(f') = m\mathtt{lm}(s \cdot h) = m(s \cdot \mathtt{lm}(h))$. From $f' \in J_d \cap V$ and $\sqrt{\nu_h} = 1^n, n \in \mathbb{N}$, it follows that $\nu_h = 1^n$, that is $h \in H \cap V$. This implies that $\mathtt{lm}(f') = m(s \cdot \mathtt{lm}(h)) = m_1(s \cdot \mathtt{lm}(h))((s+n) \cdot m_2)$, where $m_1, m_2 \in [\mathbf{X} \mid P] \cap V$ and $s = \mathrm{tdeg}(m_1)$. Since the orderings are compatible with ι, we obtain that $\mathtt{lm}(f) = w_1\mathtt{lm}(g)w_2$, where $g = \iota^{-1} = (H), w_i = \iota^{-1}(m_i)$. q.e.d.

To conclude the section we present the algorithm. For further notes on termination and correctness we refer again to [LL09].

2.23 Algorithm.

Input: G_0, a homogeneous basis of a graded two-sided ideal $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$
Output: G, a homogeneous Gröbner basis of I as two-sided ideal

$H := \iota(G_0 \setminus \{0\}$
$P := \{(f, s \cdot g) \mid f, g \in H, s \in \mathbb{N}, f \neq s \cdot g, \gcd(\mathtt{lm}(f), \mathtt{lm}(s \cdot g)) \neq 1,$
$\quad \mathtt{lcm}(\mathtt{lm}(f), \mathtt{lm}(s \cdot g)) \in V\}$
while $P \neq \emptyset$ **do**
  choose $(f, s \cdot g) \in P$
  $P := P \setminus \{(f, s \cdot g)\}$
  $h := \textsc{Reduce}(s(f, s \cdot g), \bigcup_{t\in\mathbb{N}} t \cdot H)$
  if $h \neq 0$ **then**
    $P := P \cup \{(h, s \cdot g) \mid g \in H, s \in \mathbb{N}, \gcd(\mathtt{lm}(h), \mathtt{lm}(s \cdot g)) \neq 1,$
    $\quad \mathtt{lcm}(\mathtt{lm}(h), \mathtt{lm}(s \cdot g)) \in V\}$
    $P := P \cup \{(g, s \cdot h) \mid g \in H, s \in \mathbb{N}, \gcd(\mathtt{lm}(g), \mathtt{lm}(s \cdot h)) \neq 1,$
    $\quad \mathtt{lcm}(\mathtt{lm}(g), \mathtt{lm}(s \cdot h)) \in V\}$
    $H := H \cup \{h\}$
  end if
end while
$G := \iota^{-1}(H)$
return G

The procedure Reduce mentioned in the algorithm is the classical commutative reduction. Note that this algorithm is a Buchberger type algorithm and the well-known criteria to avoid superfluous computations can be applied.

2.2 La Scala's Approach to Extend the Letterplace Correspondence

In a recent paper Roberto La Scala introduced a way to compute non-homogeneous Gröbner bases via homogenization. In this chapter we introduce his approach briefly, following along the lines of [Sca12].

First let us introduce the notion of homogenization for the free algebra $\mathbb{K}\langle\mathbf{X}\rangle$. As before we consider $\mathbf{X} = \{x_1, x_2 \ldots\}$ and we set $\overline{\mathbf{X}} = \mathbf{X} \cup \{h\}$ with h being a new variable. Then we have a natural endomorphism $\varphi : \mathbb{K}\langle\mathbf{X}, h\rangle \to \mathbb{K}\langle\mathbf{X}, h\rangle : x_i \mapsto x_i,\ h \mapsto 1$ and it is easy to see that $\mathtt{Im}(\varphi) = \mathbb{K}\langle\mathbf{X}\rangle$, so φ is a projection onto the free algebra with $\ker(\varphi) = \langle h - 1\rangle$. We call φ the dehomogenization map.

2.24 Proposition. Denote by C the largest graded ideal contained in $\ker(\varphi)$ that is $C := \{f \in \mathbb{K}\langle\mathbf{X}, h\rangle \mid f \in \ker(\varphi), f \text{ homogeneous}\}$. Then C is generated by the commutators $[x_i, h] := x_i h - h x_i$.

Proof: Clearly we have $[x_i, h] \in C$. Set $E = \{[x_i, h] \mid x_i \in \mathbf{X}\}$ and take $f \in C$. We need to show that f reduces to zero with respect to E. Obviously we have $f \equiv f' = h^{d'} \sum_k f_k h^{d-k}$, where $\mathrm{tdeg}(f) = d$, $\mathrm{tdeg}(f_k) = k$, $f_k \in \mathbb{K}\langle\mathbf{X}\rangle$ homogeneous for all k and $d' \geq 0$. Then $0 = \varphi(f) = \varphi(f') = \sum_k f_k$ and hence $f_k = 0\ \forall k$, which implies $f' = 0$. q.e.d.

This proposition allows us to define the homogenization of an ideal as well as the homogenization of a polynomial.

2.25 Definition.

- Let $f \in \mathbb{K}\langle\mathbf{X}\rangle \setminus \{0\}$ with $\mathrm{tdeg}(f) = d$ and say $f = \sum_k f_k$ is a decomposition of f into homogeneous components. We call $f^h = \sum_k f_k h^{d-k}$ the *homogenization* of f.
- Let $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$. We set I^h to be the largest graded ideal contained in $\varphi^{-1}(I)$ that is I^h is generated by all homogeneous elements in $\varphi^{-1}(I)$. We call I^h the *homogenization* of I and we have $C \subseteq I^h$.

2.26 Remark. For $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ we have $I^h = \langle f^h \mid f \in I\rangle + C$ and $\varphi(I^h) = I$.

2.27 Definition. Let $J \trianglelefteq \mathbb{K}\langle\mathbf{X}, h\rangle$ be a graded ideal containing C. We call $\mathtt{Sat}(J) := (\varphi(J))^h$ the *saturation* of J. We have $J \subseteq \mathtt{Sat}(J) \trianglelefteq \mathbb{K}\langle\mathbf{X}, h\rangle$. We call J *saturated* if $J = \mathtt{Sat}(J)$.

Note that there are more characterizations for saturations and homogenizations and we refer the interested reader to [Sca12]. For our purpose we are satisfied with the basic setup and we study analogues for the letterplace ring.

Recall that we have a multigrading on $\mathbb{K}[\mathbf{X} \mid P]$ and for any $f \in \mathbb{K}[\mathbf{X} \mid P]$ we can build the decomposition $f = \sum_{\mu} f_\mu$ into its *multi-homogenous* elements. This allows us to translate our methods above to the letterplace ring.

2.28 Definition. Consider the endomorphism $\mathbb{K}[\mathbf{X}, h \mid \mathbb{N}]$ and $\psi : \mathbb{K}[\mathbf{X}, h \mid \mathbb{N}] \to \mathbb{K}[\mathbf{X}, h \mid \mathbb{N}] : \ x_i(s) \mapsto x_1(s), \ h(s) \mapsto 1 \quad \forall s \in \mathbb{N}$. One has $\ker(\psi) = \langle \{h(s) - 1 \mid s \in \mathbb{N}\} \rangle$.

- Let $f \in \mathbb{K}[\mathbf{X} \mid P] \setminus \{0\}$ with $\mathrm{tdeg}(f) = d$ and say $f = \sum_{\mu} f_\mu$ is a decomposition of f into multi-homogeneous components. We call $f^h = \sum_{\mu} f_\mu \prod_{k=|\mu|+1}^{d} h(k)$ the *multi-homogenization* of f.
- Let $J \trianglelefteq \mathbb{K}[\mathbf{X} \mid P]$. We set J^h to be the largest graded ideal contained in $\psi^{-1}(J)$ that is J^h is generated by all homogeneous elements in $\psi^{-1}(J)$. We call J^h the *multi-homogenization* of J.
- Let $J \trianglelefteq \mathbb{K}[\mathbf{X}, h \mid \mathbb{N}]$ be a multigraded ideal. Define $\mathtt{Sat}(J) = (\psi(J))^h$. We call $\mathtt{Sat}(J)$ the saturation of J.

We will assume that our ordering is compatible with ι as well as shift-compatible that is $m < s \cdot m \ \forall m \in [\mathbf{X} \mid \mathbb{N}], s \in \mathbb{N}$.

2.29 Remark. It is important to note that the elements $\bar{\iota}([x_i, h]) = x_i(1)h(2) - h(1)x_i(2)$ for $i \geq 1$ form a Gröbner shift basis of the ideal $D := \bar{\iota}(C)$. We say $G \subset J \cap V^h$ is a Gröbner letterplace basis of J modulo D if $G \cup \{\bar{\iota}([x_i, h]) \mid i \geq 1\}$ is a Gröbner letterplace basis of J.
Let $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$ be an arbitrary ideal and let G be any Gröbner basis of I. Then G^h is a Gröbner basis of I^h and $\mathtt{lm}(G) = \mathtt{lm}(G^h)$. We translate this basic idea now to the letterplace realm.

2.30 Proposition.
- Let $J \subset \mathbb{K}[\mathbf{X}, h \mid \mathbb{N}]$ be a letterplace ideal containing D. Then a Gröbner letterplace basis of $\mathtt{Sat}(J)$ modulo D is given by the elements $(\psi(f))^h \ \forall f \in J \cap V^h$, where f is in normal form with respect to D.
- Let $J \subset \mathbb{K}[\mathbf{X}, h \mid \mathbb{N}]$ be a letterplace ideal containing D and set $J' = \mathtt{Sat}(J)$. Moreover, let G be a Gröbner letterplace basis of J modulo D. Then $G' = (\psi(G))^h$ is a Gröbner letterplace basis of J' modulo D.

Proof: [Sca12], Proposition 5.8 and 5.9

From those results one immediately obtains an algorithm for computing Gröbner bases using the correspondence for homogenized generating sets.

2.31 Algorithm. Input: H, a generating set of an ideal $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$
Output: $\varphi(\bar{\iota}^{-1}(G))$, a Gröbner basis of I

$G := \bar{\iota}(H^h \cup \{[t, x_i] \mid i \geq 1\})$
$B := \{(f, g) \mid f, g \in G\}$
while $B \neq \emptyset$ **do**
  choose $(f, g) \in B$
  $B := B \setminus \{(f, g)\}$
  for all $i > 0$ s.t. $\gcd(\mathtt{lm}(f), \mathtt{lm}(i \cdot g)) \neq 1$, $\mathtt{lcm}(\mathtt{lm}(f), \mathtt{lm}(i \cdot g)) \in V^h$ **do**
    $s := \textsc{Reduce}(s(f, i \cdot g), \mathbb{N} \cdot G)$
    if $s \neq 0$ **then**
      $s := (\psi(s))^h$
      $B := B \cup \{(s, s), (s, k), (k, s) \mid k \in G\}$
      $G := G \cup \{h\}$
    end if
  end for
end while
return $\varphi(\bar{\iota}^{-1}(G))$

2.32 Remark. If I has a finite Gröbner basis then the algorithm is able to compute it in a finite number of steps. However, termination is not guaranteed and the results of adding a degree bound mentioned earlier apply.

We like to point out that it is possible to optimize the procedure by using a smallest homogenization in each step, that is no leading monomial of any element should contain any shift of $\iota(h)$, thereby decreasing the total degree of polynomials. The procedure is introduced and explained in [Sca12].

Notably, Ufnarovskij presented in [Ufn08] a neat method for homogenization of generators of ideals in $\mathbb{K}\langle \mathbf{X} \rangle$ and computations of Gröbner bases of those ideals. Those methods are implemented in the computer algebra system Bergman ([B$^+$06]).

2.3 Place Grading

While being algorithmically feasible in the Noetherian case, the computation of a Gröbner basis of a non-graded ideal in the non-Noetherian case has the following problem: A non-graded ideal $I \in \mathbb{K}\langle \mathbf{X} \rangle$ may have a finite Gröbner basis, while a homogenized set of generators leads to an infinite Gröbner basis.
Our goal is to show that introducing a new variable is superfluous. In fact one can use the structure given by the letterplace ring quite successfully. Therefore we present a new way to grade letterplace ideals.

2.33 Definition. We call the *place support* of $m \in [\mathbf{X} \mid P]$ the set of places occurring in m. A monomial m is called *place-multi-linear*, if each number from

the place support occurs at most once, that is monomials of $[\mathbf{X} \mid P]$, whose place support is irredundant as a set.

2.34 Definition.

- Denote by $W' \subset \mathbb{K}[\mathbf{X} \mid P]$ the vector space, spanned by all place-multi-linear monomials. Let $W \subset W'$ be spanned by all place-multi-linear monomials of shift zero.
- For a monomial $m \in W$, define the **place-degree** $\mathtt{pdeg}(m)$ to be the highest place occurring in the place-support of m and we set $\mathtt{pdeg}(m) = 0$ for $m \in \mathbb{K}$ by convention. For a polynomial $p \in W \setminus \{0\}$ we set $\mathtt{pdeg}(p) = \max_i\{\mathtt{pdeg}(m_i) | p = \sum a_i m_i, a_i \in \mathbb{K} \setminus \{0\}\}$.
- If there is $1 \leq k \leq \mathtt{pdeg}(m)$, such that k is not in the place-support, we say that m has a *hole* at place k. The number of holes between the first occurring variable and the last one is called the **place defect** of m.
- Let $\cdot_{lp}$ be the *letterplace multiplication* on $\mathbb{K}[\mathbf{X} \mid P]$, that is $m_1 \cdot_{lp} m_2 = m_1(\mathtt{pdeg}(m_1) \cdot m_2)$ for polynomials $m_1, m_2 \in \mathbb{K}[\mathbf{X} \mid P]$.
- Define $W_k = \{w \in W \mid \mathtt{pdeg}(w) = k\} \subseteq W$.

We start with some easy properties of the place-degree. Recall the definition of V and V' (2.5).

2.35 Proposition. The following holds:

1. $W' = \bigcup_{s \in \mathbb{N}_0} s \cdot W$.
2. $\mathtt{pdeg}(m_1 \cdot_{lp} m_2) = \mathtt{pdeg}(m_1) + \mathtt{pdeg}(m_2) = \mathtt{pdeg}(m_2 \cdot_{lp} m_1)$ and thus $W_l \cdot_{lp} W_k \subseteq W_{l+k}\ \forall l, k \in \mathbb{N}_0$.
3. $\forall m \in W'$: $\mathtt{pdeg}(m) = \mathrm{tdeg}(m) + \mathtt{shift}(m) +$ place-defect(m).
4. $W = \bigoplus_{k \in \mathbb{N}_0} W_k$ is graded with respect to place-degree. The same holds for W'.
5. $V_0 = W_0 = \mathbb{K}$, $V_1 = W_1 = \oplus_{i=1}^n \mathbb{K}x_i(1)$ and $V_k \subsetneq W_k\ \forall k \geq 2$. Thus $V \subsetneq W$ and $V' \subsetneq W'$.
6. Place grading respects shifts, that is $s \cdot W_k \subset W_{k+s}\ \forall k, s \in \mathbb{N}$ holds.

Proof:

1. Each monomial $m \in [\mathbf{X} \mid P]$ with $\mathtt{shift}(m) = k$ is the image of some monomial $\tilde{m} \in [\mathbf{X} \mid P]$ with $\mathtt{shift}(\tilde{m}) = 0$ under the shift action.

2. Obviously we have $\texttt{pdeg}(k \cdot m) = k + \texttt{pdeg}(m)$ and thus the claim follows by definition of $\cdot_{lp}$.

3. Since $m \in W'$ we have that $\mathrm{tdeg}(m)$ equals the number of places occupied by a variable.

4. Clearly we have $W_k \cap W_l = \emptyset \; \forall k \neq l$ and if B_{W_k} is a monomial basis for W_k we have that $\bigcup_{k \in \mathbb{N}_0} B_{W_k}$ is a monomial basis for W.

5. Clear by definition.

6. Follows immediately from 2. q.e.d.

2.36 Example. To get a deeper insight into the structure of W a look into the graded parts is useful. It is easy to see that $W_0 = K \cdot \{1\} = V_0$ and $W_1 = K \cdot \{x_i \mid 1 \leq i \leq n\} = V_1$. According to the definition, $W_2 = V_2 \oplus (1 \cdot V_1)$. Further on, we find $W_3 = V_3 \oplus (1 \cdot W_2) \oplus (W_1 \times 2 \cdot W_1)$, where $W_1 \times 2 \cdot W_1 = \{w(2 \cdot \tilde{w}) \mid w, \tilde{w} \in W_1\}$. Substituting previous expressions we obtain $W_3 = V_3 \oplus (1 \cdot V_2) \oplus (2 \cdot V_1) \oplus (V_1 \times 2 \cdot V_1)$.

It is important to note that W and W' are both graded vector spaces using the place grading. So one can use this to homogenize arbitrary polynomials by places.

2.37 Definition. Let $G \subset \mathbb{K}\langle \mathbf{X} \rangle$ be a set of polynomials and put $\tilde{G} = \iota(G) \subset \mathbb{K}[\mathbf{X} \mid P]$. Then for each $\tilde{p} = \sum_i a_i \tilde{m}_i \in \tilde{G}$ with $a_i \in \mathbb{K} \setminus \{0\}, \tilde{m}_i \in [\mathbf{X} \mid P]$ we set

$$p_h = \sum_i a_i (\texttt{pdeg}(\tilde{p}) - \texttt{pdeg}(m_i)) \cdot m_i \in \mathbb{K}[\mathbf{X} \mid P].$$

Then p_h is graded with respect to place-degree or *place-homogeneous*. We call p_h the *place-homogenization* of $\tilde{p}$.

The idea behind place-homogenization is to avoid adding a new variable to the free algebra, since one is able to use places to homogenize polynomials. Let us consider an easy example.

2.38 Example. Consider $\mathbb{K}\langle x, y \rangle$ and take $p = xyx + xy + y$. Then $\tilde{p} := \iota(p) = x(1)y(2)x(3) + x(1)y(2) + y(1) \in K[x, y \mid \mathbb{N}]$, which is clearly not homogeneous. We then have $\tilde{p}_h = x(1)y(2)x(3) + x(2)y(3) + y(3)$ as the place-homogenization of $\tilde{p}$.

Sadly $\tilde{p}_h$ is not even in V', which makes it harder to recognize as an element in the free algebra, since the direct correspondence can not be applied. Things get even worse when multiplication is applied, even if we use the letterplace multiplication $\cdot_{lp}$.

2.39 Example. As before we take $\tilde{p} := x(1)y(2)x(3) + x(1)y(2) + y(1) \in K[x, y \mid \mathbb{N}]$ and its place-homogenization $\tilde{p}_h$. If we post-multiply $x(1)$ we get $\tilde{p}_h \cdot_{lp} x(1) = x(1)y(2)x(3)x(4) + x(2)y(3)x(4) + y(3)x(4)$, which is place-homogeneous and of a similar shape as $\tilde{p}_h$. Now, if we pre-multiply $x(1)$ we get $x(1) \cdot_{lp} \tilde{p}_h = x(1)x(2)y(3)x(4) + x(1)x(3)y(4) + x(1)y(4)$, which is still place-homogeneous. However, it contains proper holes, that is some monomials have positive place-defect. On the bright side we have that $\tilde{p}_h \cdot_{lp} x(1), x(1) \cdot_{lp} \tilde{p}_h \in W'$. But since those elements are not necessarily in an orbit with an element of V under the shift-action, it is hard to recognize the corresponding element in the free algebra, which should be the goal of the dehomogenization.

2.40 Definition. Define a $\mathbb{K}$-linear map $\texttt{shrink} : W' \to V$ as follows:
• For $m \in V$, $\texttt{shrink}(m) := m$.
• For $m \in W' \setminus V$, one has the following:

- $1 \leq \deg(m) = d$ and $\texttt{pdeg}(m) = d' > d$, so $s_d := d' - d \geq 1$
- $\exists s_1, \ldots, s_{d-1} \in \mathbb{N}_0$ such that $m = (s_1 \cdot x_{i_1}(1)) \cdots (s_d \cdot x_{i_d}(d))$.

We set $\texttt{shrink}(m) := x_{i_1}(1) \cdots x_{i_d}(d) \in V$.

2.41 Remark. The map `shrink` is a well-defined homomorphism of vector spaces and for an element $m \in W'$ it returns the unique element $\tilde{m} \in V$ with $shift(\tilde{m}) = 0$ containing the same word of letters as m. Note that it can be extended to non place-linear monomials, in which case `shrink` just closes holes in the monomial and sets the shift to zero.
To see that it is of good value for our efforts we consider the example from above.

2.42 Example. In the same setup as before we have

$$\texttt{shrink}(\tilde{p}_h \cdot_{lp} x(1)) = x(1)y(2)x(3)x(4) + x(1)y(2)x(3) + y(1)x(2)$$

and

$$\texttt{shrink}(x(1) \cdot_{lp} \tilde{p}_h) = x(1)x(2)y(3)x(4) + x(1)x(2)y(3) + x(1)y(2).$$

It is easy to see that $px = \iota^{-1}(\texttt{shrink}(\tilde{p}_h \cdot_{lp} x(1)))$ and $xp = \iota^{-1}(\texttt{shrink}(x(1) \cdot_{lp} \tilde{p}_h))$ holds.

The example motivates the following definition.

2.43 Definition. Define an equivalence relation on W' by $m_1 \sim m_2 \Leftrightarrow \texttt{shrink}(m_1) = \texttt{shrink}(m_2)$. Moreover, define a map $\star : V \times V \to W'/\!\sim$: $(v_1, v_2) \mapsto [v_1(\texttt{pdeg}(v_1) \cdot v_2)]$.

2.44 Remark. Since `shrink` is a homomorphism of vector spaces it is clear that the relation defined above is an equivalence relation and $V \cong W'/\!\sim \cong W'/\ker(\texttt{shrink})$.
To see that $\star$ is well-defined one needs to check that it is independent from the choice of the representative of a residue class. Note that for $v, w \in V$ we have $v(\texttt{pdeg}(v) \cdot w) = v \cdot_{lp} w \in W'$ and therefore $\texttt{shrink}(v(\texttt{pdeg}(v) \cdot w)) = \iota(\iota^{-1}(v)\iota^{-1}(w))$. Now for $v', w' \in W'$ such that $[v] = [v'], [w] = [w']$ we get $\texttt{shrink}(v'(\texttt{pdeg}(v') \cdot w')) = \texttt{shrink}(\texttt{shrink}(v')(\texttt{pdeg}(v') \cdot \texttt{shrink}(w'))) =$
$\texttt{shrink}(v(\texttt{pdeg}(v') \cdot w) = \texttt{shrink}(v(\texttt{pdeg}(v') \cdot w)$, which proves the claim. To see that the last equality holds note that $\texttt{shrink}(v_1(s \cdot v_2)) = \texttt{shrink}(v_1(s' \cdot v_2))\ \forall v_1, v_2 \in V, s, s' \geq \texttt{pdeg}(v_1)$.

2.45 Lemma. Define a $\mathbb{K}$-linear map

$$\eta : V \to W'/\!\sim, \quad f = \sum_i a_i m_i \mapsto [f].$$

Then η is an isomorphism of vector spaces with `shrink` being the inverse map.

Proof: Since V is stable under shrinking, η is injective. Let $w \in W'$ be place-multi-linear, then $\texttt{shrink}(w) \in V$ belongs to $[w]$ and thus η is surjective. q.e.d.

If we identify a residue class $[w] \in W'/\!\sim$ with the unique element $v \in V$ contained in this class we can think of $\star$ as a multiplication on V, which respects the total degree of polynomials, thus giving V a $\mathbb{K}$-algebra structure.

2.46 Lemma.
Define the map $\star : V \times V \to V :\ (v_1, v_2) \mapsto \texttt{shrink}(v_1(\texttt{pdeg}(v_1) \cdot v_2))$.

1. $\star$ is $\mathbb{K}$-bilinear.
2. We have $p \star q = 0 \ \Leftrightarrow\ p = 0 \vee q = 0$.
3. $\star$ is associative.

Proof:

1. Recall that `pdeg` of a polynomial is the highest occurring place in any monomial with non-zero coefficient. Again, we have $\texttt{shrink}(v_1(s \cdot v_2)) = \texttt{shrink}(v_1(s' \cdot v_2))\ \forall v_1, v_2 \in V, s, s' \geq \texttt{pdeg}(v_1)$. The claim follows by the linearity of `shrink`, shift and the multiplication on $\mathbb{K}[\mathbf{X} \mid P]$ as a ring.

2. Because we have $p \star q = (\sum_d^D p_d) \star (\sum_e^E q_e) =$
$\sum_{k=0}^{D+E} (\sum_{d=0}^{k} p_d q_{k-d})$, where p_d, q_e are `pdeg`$-$graded components of p and q respectively we need to prove the claim for `pdeg`-graded components $\sum_d p_d q_{k-d}$

only. Because $p, q \in V$ we have that $\sum_d p_d q_{k-d}$ is homogeneous and the claim follows by the fact, that we can use the letterplace multiplication for the graded case, since we have $\mathtt{shrink}(p(\mathtt{pdeg}(p) \cdot q)) = p(\mathtt{pdeg}(p) \cdot q)$.

3. With the same argument as before we need to show associativity for homogeneous components only. So take $p_d, q_e, w_k \in V$ homogeneous. Then $p_d \star (q_e \star w_k) = p_d(d \cdot (q_e(e \cdot w_k))) = p_d(d \cdot q_e)((d+e) \cdot w_k) = (p_d \star q_e) \star w_k$. q.e.d.

2.47 Corollary. The map $\star$ induces a multiplication on V, thus $(V, +, \star)$ is a $\mathbb{K}$-algebra.

Proof: Since we already know that $(V, +)$ is a vector space all we have to do is to check distributivity and associativity, both following immediately from 2.46. q.e.d.

Indeed the map $\star$ can be extended to a map $\mathbb{K}[\mathbf{X} \mid P] \times \mathbb{K}[\mathbf{X} \mid P] \to V$, which enjoys similar properties.

2.48 Theorem. Define a $\mathbb{K}$-linear map $\vartheta : (\mathbb{K}\langle \mathbf{X} \rangle, \cdot) \to (V, \star) : p = \sum_j c_j m_j \mapsto \sum_j c_j \iota(m_j)$. Then ϑ is a $\mathbb{K}$-algebra isomorphism.

Proof: By definition ϑ is $\mathbb{K}$-linear and we have $\vartheta(p + q) = \vartheta(p) + \vartheta(q)\ \forall p, q \in \mathbb{K}\langle \mathbf{X} \rangle$. We need to show that $\vartheta(p \cdot q) = \vartheta(p) \star \vartheta(q)\ \forall p, q \in \mathbb{K}\langle \mathbf{X} \rangle$. We have $\vartheta(p) \star \vartheta(q) = \vartheta(\sum_i a_i p_i) \star \vartheta(\sum_j b_j q_j) = \sum_{i,j} a_i b_i \vartheta(p_i) \star \vartheta(q_j)$. Because $\vartheta(p_i) \star \vartheta(q_j) = \iota(p_i) \star \iota(q_j) = \mathtt{shrink}(\iota(p_i)(\mathrm{tdeg}(p) \cdot \iota(q_j))) = \iota(p_i)(\mathrm{tdeg}(p_i) \cdot \iota(q_j)) = \iota(p_i q_j)$, where we used the remark given in the proof of 2.46, we have $\vartheta(p) \star \vartheta(q) = \sum_{i,j} a_i b_i \iota(p_i q_j) = \sum_{i,j} a_i b_i \vartheta(p_i q_j) = \vartheta(p \cdot q)$ using linearity of ϑ.
Because of 2.46 (2) ϑ is injective. Since V is defined as the image of ι we have that ϑ is also surjective, which completes the proof. q.e.d.

2.49 Remark. Take an ideal $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$. The set $J = \vartheta(I)$ is also an ideal in V with respect to the new multiplication $\star$ and because of the properties of ϑ the feature of a subset being a generating system or even a Gröbner basis translates. However, J is not an ideal of $\mathbb{K}[\mathbf{X} \mid P]$ with respect to the standard multiplication of $\mathbb{K}[\mathbf{X} \mid P]$. So the question arises if there is a correspondence similar to the one in [LL09], which we will discuss further at the end of the next section.

Knowing about the problem behind homogenization mentioned earlier there are steps one can take in order to avoid it. One has to apply an ordering which allows one to simplify the homogenization in each step, thereby reducing the maximal degree of the homogenized truncated Gröbner bases in each step. This is known as *saturation on the fly* and is also briefly discussed in [Sca12].

By using graded techniques on the homogenized ideal, our aim is not to compute the trusted homogenized ideal, but to come as directly as possible to the non-graded Gröbner basis, which is usually obtained via the post-computation of the saturation.

We like to point out the difference between our new approach and classical homogenization. As the first step let us recall the homogenization.

2.50 Definition. Consider the free algebra $\mathbb{K}\langle\mathbf{X}\rangle$ and let h be a new variable commuting with all $x_i \in \mathbf{X}$. Define $\overline{\mathbf{X}} = \mathbf{X} \cup \{h\}$ and $F = \mathbb{K}\langle\overline{\mathbf{X}}\rangle$. Then each $p \in \mathbb{K}\langle\mathbf{X}\rangle$ is the image of some homogeneous element $\overline{p} \in \mathbb{K}\langle\overline{\mathbf{X}}\rangle$ under the algebra homomorphism Φ defined via $\Phi(x_i) = x_i,\ \Phi(h) = 1$. More precisely, if we have $f = \sum_{k=0}^{d} p_k$ with $p_k \in \mathbb{K}\langle\mathbf{X}\rangle_k,\ p_d \neq 0$, then $\tilde{p} = \sum_{k=0}^{d} p_k h^{d-k}$ is a homogeneous polynomial with $\Phi(\tilde{p}) = p$.

2.51 Remark. In order to compute a Gröbner basis via classical homogenization one has to employ an ordering that has the following property: $h^k \mid \mathtt{lm}(\tilde{p})$ then h^k divides each term occurring in $\tilde{p}$ with non-zero coefficient. An example for such an ordering was introduced earlier (see 1.29) and can be found in [Li12] and in [BB98] as well as in [Mor88] and there is a full introduction to this topic. In particular, note that for a properly homogenized polynomial $\tilde{p}$ we always have $h \nmid \mathtt{lm}(p)$ with respect to such an ordering.
After one has computed the Gröbner basis of a homogenized ideal, a saturation of the result with respect to h must be computed. If we introduce the commutators to the homogenized ideal one is always able to *move* the homogenization variable to the end of each monomial using reduction if needed. Indeed, for each computed S-polynomial p, such that $h^k | \mathtt{lm}(p)$, one can replace p with the polynomial p/h^k. This procedure is called *saturation on the fly*, because p/h^k belongs to the saturated homogenized ideal. This allows one to reduce significantly the total degree of considered polynomials during the computation. Note that the somewhat analogous effect in the commutative case can be achieved by using the notion of *ecart* (see for example [GP08]).

Recognizing holes as traces of the homogenization, one can apply the method presented by La Scala rather effectively. The big advantage hereby is that one does not need to introduce an extra variable and in each step of the algorithm a sort of saturation-on-the-fly is applied. Also, it is not necessary to choose a special ordering for the homogenization variable.

Note that the classical operations with polynomials (creation of S-polynomials, reductions etc.) usually produce holes in the monomials of inhomogeneous input. Hence we need to introduce a new reduction routine Shrink-Reduce, which applies shrinking after each elementary reduction step $f = f - c_i m_i h$, where h is a reductor, $c_i \in \mathbb{K}$ and $m_i \in V$.

2.52 Algorithm.

Input: $f = \sum_{j=1}^{d} c_j t_j \in V$, $\{h_1, \ldots, h_k\} \subset V$, $k \in \mathbb{N}$

Output: $r \in V$, such that $f = \sum_i c_i m_i h_i + r$ and $\mathtt{lm}(h_i) \nmid r \; \forall 1 \leq i \leq k$

Set $\tilde{f} = f$.
while $\exists s, i, j \in \mathbb{N} : \; c(s \cdot \mathtt{lm}(h_i)) = t_i$ for some $c \in \mathbb{K}[\mathbf{X} \mid P]$ **do**
$\tilde{f} = \tilde{f} - c(s \cdot h_i)$
$\tilde{f} = \mathtt{shrink}(\tilde{f})$
end while
return $\tilde{f}$

Equipped with this new procedure we are now able to state a full algorithm that can compute Gröbner bases.

2.53 Algorithm.

Input: G_0, a generating set of an ideal $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$
Output: G, a Gröbner basis for I

$H := \iota(G_0 \setminus \{0\})$;
$P = \{(f, s \cdot g) \mid f, g \in H, s \in \mathbb{N}, f \neq s \cdot g, \gcd(\mathtt{lm}(f), \mathtt{lm}(s \cdot g)) \neq 1,$
$\mathtt{lcm}(\mathtt{lm}(f), \mathtt{lm}(s \cdot g)) \in V\}$;
while $P \neq \emptyset$ **do**
Choose $(f, s \cdot g) \in P$;
$P = P \setminus (f, s \cdot g)$;
$h :=$ Shrink-Reduce($\mathtt{shrink}(S(f, s \cdot g)), H$);
if $h \neq 0$ **then**
$P := P \cup \{(h, s \cdot g) \mid g \in H, s \in \mathbb{N}, \gcd(\mathtt{lm}(h), \mathtt{lm}(s \cdot g)) \neq 1, \mathtt{lcm}(\mathtt{lm}(h), \mathtt{lm}(s \cdot g)) \in V\}$;
$P := P \cup \{(g, s \cdot h) \mid g \in H, s \in \mathbb{N}, \gcd(\mathtt{lm}(g), \mathtt{lm}(s \cdot h)) \neq 1, \mathtt{lcm}(\mathtt{lm}(g), \mathtt{lm}(s \cdot h)) \in V\}$;
$H := H \cup \{h\}$;
end if
end while;
$G := \iota^{-1}(H)$;
return G;

2.54 Theorem. If the algorithm above terminates it returns a reduced Gröbner basis for the ideal I.

Proof: As explained before we can associate I to an ideal $\tilde{I}$ in $(V, \star)$. Then H is a generating system for $\tilde{I}$. Moreover, $\vartheta(H)$ can be viewed as a set of residue classes and identified with the place homogenization of those elements. Since leading monomials are not affected by the homogenization P clearly contains all critical pairs, as shown in the proof for graded ideals in [LL09].
So the only thing to prove is the correctness of the computation of h. Therefore

we observe that the computations of $\texttt{shrink}(S(f, s \cdot g))$ relates to the pre- and post-multiplication of the cofactors using the $\star$-multiplication and the same holds for the procedure Shrink-Reduce. Therefore we can view h as an S-polynomial of a Gröbner basis computation in $(V, \star)$ and the correctness of the Buchberger procedure completes the proof. q.e.d.

2.55 Remark. In general, the termination is not guaranteed, however it can be achieved by adding a degree bound as usual. In the homogeneous case the output is a subset of the full reduced Gröbner basis, but in the general case this is not clear. However, it will be part of some (not necessarily reduced) Gröbner basis and thus the set may have some uses. For a detailed view on partial and truncated Gröbner bases we refer to [Stu10], but we will see some of the uses in the next chapter.

As stated before we have a direct correspondence between ideals in $\mathbb{K}\langle\mathbf{X}\rangle$ and ideals in $(V, \star)$, which also gives a direct correspondence between generating sets and Gröbner bases. Recall that for a graded, two-sided ideal $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ we call the ideal $J \trianglelefteq \mathbb{K}[\mathbf{X} \mid P]$ generated by $\bigcup_{s\in\mathbb{N}} s \cdot \iota(I)$ the *letterplace analogue* of I. On the other hand we have for a graded, shift-invariant ideal $J \trianglelefteq \mathbb{K}[\mathbf{X} \mid P]$ an ideal $\iota^{-1}(J) := I := \iota^{-1}(J \cap V)$.
Now if we drop the assumption that our ideals are graded we still have $I = \iota^{-1}(\iota(I))$ but in general we only get $\iota(\iota^{-1}(J)) \subseteq J$ (see [LL09] Proposition 2.9). For a general ideal $J \trianglelefteq \mathbb{K}[\mathbf{X} \mid P]$ equality can never be achieved, as the examples $J := \langle x(2)x(4)\rangle \trianglelefteq \mathbb{K}[x \mid \mathbb{N}]$ shows: Here $J \cap V = \{0\}$ and hence $\iota(\iota^{-1}(J)) = \{0\}$. For generating sets consider $x^2 + x \in \mathbb{K}\langle x, y\rangle$. Then $x^2y + xy \in \langle x^2 + x\rangle$, but $x(1)x(2)y(3) + x(1)y(2) \notin \langle \bigcup_{s\in\mathbb{N}} s \cdot (x(1)x(2) + x(1))\rangle \trianglelefteq \mathbb{K}[x, y \mid \mathbb{N}]$. Even if we choose $x(1)x(2) + x(2)$ as the representative of $\iota(x^2 + x)$ and take $\langle \bigcup_{s\in\mathbb{N}} s \cdot (x(1)x(2) + x(2))\rangle$ and thus considering a place-homogeneous ideal we have a similar problem with $yx^2 + yx \in \langle x^2 + x\rangle$. To avoid this problem the usage of shrinking is needed, which in turn leads to the $\star$-multiplication. Therefore, a classical correspondence of generating sets or even Gröbner bases like in the graded case can not be achieved by only using the natural multiplication of $\mathbb{K}[\mathbf{X} \mid P]$ or the letterplace multiplication.

2.4 A new Invariant for the Shift-Action

In this section we intend to find a better way to handle monomials and their shifts over the letterplace ring. For that we investigate the monoid action of $\mathbb{N}$ and especially the orbits of the elements of V.

2.56 Remark. Note that the image of V under the action of $\mathbb{N}$ is exactly the vector space V'. This follows immediately by the definition of V' (2.5).

Furthermore, for each $m \in V$ we have $\mathbb{N} \cdot m = \{s \cdot m \mid s \in \mathbb{N}\}$, that is an orbit consists of a monomial and all its shifts. So whenever we need to choose a representative for one of these orbits we will take the one with shift zero.

Since $\mathbb{K}[\mathbf{X} \mid P]$ is a commutative polynomial ring one can introduce the notion of exponent vectors. However, since $\mathbb{K}[\mathbf{X} \mid P]$ is not finitely generated this vector has infinitely many entries. This problem can be avoided since each monomial has finite support and we can cut all zeros at the end of the vector.

2.57 Remark. Take $m \in V' \subset \mathbb{K}[x_1, \ldots, x_n \mid \mathbb{N}]$ with $\deg(m) = d$ and $\texttt{shift}(m) = s$. The classical exponent vector $\alpha \in \mathbb{N}_0^{n(d+s)}$ has the property

$$m = x_1(1)^{\alpha_1} x_2(1)^{\alpha_2} \cdots x_n(1)^{\alpha_n} \cdot x_1(2)^{\alpha_{n+1}} \cdots x_n(2)^{\alpha_{2n}} \cdots$$

One can write $\alpha = (e_1, \ldots, e_{d+s})$ with vectors $e_i \in \mathbb{N}^n$, such that

- For $1 \leq i < s$, e_i is zero vector.
- For $i \geq s$, e_i contains exactly one 1 ($e_i[k] = 1 \Leftrightarrow x_k(i)$ divides m).

Note that the position of the 1 in the k-th block is equal to i_k. It follows that the 1 is on position j in the k-th block, if and only if $(x_j \mid k) | m$. So if one knows the positioning of all ones, one can reconstruct the monomial.

From now on, we call $(e_1, \ldots, e_{d+s})$ the *exponent vector* of m. For a vector $v = (v_1, \ldots, v_k)$ we call k the *size* or *length* of v, denoted by $\texttt{lg}(v)$.

2.58 Lemma. Let $m \in V'$, $s \in \mathbb{N}$ and $m' := s \cdot m$. Moreover, let e and e' be exponent vectors of m and m'. If $\deg(m) = d$, then by setting $\tilde{e} = (e'_s, \ldots, e'_{s+d})$ one obtains $\tilde{e} = e$.

Proof: Since $\texttt{shift}(m') \geq s$ we have $e'_i = (0, \ldots, 0)\ \forall i < s$. It follows that $\texttt{shift}(\tilde{m}) = \texttt{shift}(m') - s$ and $s \cdot \tilde{m} = m'$, which already implies $\tilde{m} = m$ and thus $\tilde{e} = e$. q.e.d.

2.59 Definition. Let $m \in V'$ with $\deg(m) = d$, $\texttt{shift}(m) = s$, exponent vector e as before and $\tilde{e} := (e_s, \ldots, e_{d+s})$. Construct the *distance vector* D of m as follows: The first entry of D is the position of the 1 occurring in e_s. For $1 < i \leq d$ the i-th entry equals one plus the number of zeros between the 1 in e_{s+i} and the 1 in e_{s+i-1}.
Denote by dv the map that assigns to each monomial $m \in V'$ its distance vector.

2.60 Proposition. The map dv is an invariant for the shift action, which separates the orbits. That is for all $m, m' \in V'$ we have: $m' = s \cdot m$ or $m = s \cdot m'$ for some $s \in \mathbb{N}$ if and only if $dv(m) = dv(m')$.

Proof: " $\Rightarrow$: " Follows immediately by the previous lemma, because the distance vector ignores the shift of an monomial, that is leading zero blocks of the exponent

vector are cut of.
" $\Leftarrow$: " It is sufficient to show that the restriction of dv to V is injective, which is clear by Remark 2.57. q.e.d.

This leads to a way to decide whether or not $m|m'$ for monomials $m, m' \in \mathbb{K}\langle \mathbf{X} \rangle$.

2.61 Definition. For two distance vectors d and d' we say that d *is contained in* d', if $\mathtt{lg}(d') \geq \mathtt{lg}(d)$ and there exists $i \in \{1, \ldots, \mathtt{lg}(d')\}$ such that $d[1] = d'[i] + i \cdot n - \sum_{j=1}^{i-1} d'[j]$ and for $1 < j \leq \mathtt{lg}(d)$ we have $d[j] = d'[i + j - 1]$.

2.62 Remark. By construction of the distance vectors we have $dv(m)$ is contained in $dv(m')$ if and only if there exists $s \in \mathbb{N}$ such that $s \cdot m | m' \qquad \forall m, m' \in \mathbb{K}[X|P]$.

2.63 Corollary. Take two monomials $m, m' \in \mathbb{K}\langle \mathbf{X} \rangle$, set $n = \iota(m), n' = \iota(m')$ and name the distance vectors d and d' respectively. Then:
$m|m' \quad \Leftrightarrow \quad d$ is contained in d'.

Proof: $m|m' \quad \Leftrightarrow \quad \exists s \in \mathbb{N} : \ s \cdot n | n'$. Since distance vectors ignore the shift this proves the claim. q.e.d.

2.64 Remark. This leads to a practical way to conclude if $m|m'$ by just comparing the distance vectors. The nice thing about this procedure is that one gets the shift s directly and can use $s \cdot n$ say for reduction of n' (or the corresponding polynomials respectively). Notably by using division for letterplace monomials one can compute $n'/(s \cdot n)$ and gets the coefficients for the reduction by applying commutative methods.

This can be used to improve the letterplace algorithm for computing Gröbner bases, since one has not to consider and store all of the shifts of n, but only check the distance vectors if they are contained in one another, thereby finding obstructions corresponding to overlaps.

2.4.1 Using the shift-invariant representation

Equipped with the knowledge that we can compute Gröbner bases of non-graded ideals using the letterplace approach without introducing direct homogenization one can ask if there is a better way, because applying shrinking to each new S-polynomial can be very costly.

Recall that one can use distance vectors to represent monomials in a shift invariant way. By switching to this new representation one can multiply monomials more effectively. Now, since distance vectors are independent of shifts, they are a natural choice to represent the equivalence class of an monomial in $W'/\!\!\sim$. First we want to see how to multiply two distance vectors correctly.

2.65 Proposition. Denote by $\mathtt{lg}$ the size of a distance vector.
Take two monomials $m_1, m_2 \in \mathbb{K}\langle \mathbf{X} \rangle$ and set $\tilde{m}_1 := \iota(m_1)$, $\tilde{m}_2 := \iota(m_2)$, $dm_1 := dv(\tilde{m})$, $dm_2 := dv(\tilde{m}_2)$. Define a new vector d by setting

$$d[1 \dots \mathtt{lg}(dm_1)] = dm_1,$$

$$d[\mathtt{lg}(dm_1) + 1] = \mathtt{lg}(dm_1)n - (\sum_{k=1}^{\mathtt{lg}(dm_1)} dm_1[k]) + dm_2[1],$$

$$d[(\mathtt{lg}(dm_1) + 2) \dots (\mathtt{lg}(dm_1) + \mathtt{lg}(dm_2))] = dm_2[2 \dots \mathtt{lg}(dm_2)].$$

Then $dv(\iota(m_1 m_2)) = d$.

Proof: To see that the claim is correct one only needs to notice that the entry $d[\mathtt{lg}(dm_1)+1]$ is exactly the gap in the exponent vector of $\tilde{m}_1 \mathtt{lg}(dm_1) \cdot \tilde{m}_2$ between the last variable of $\tilde{m}_1$ and the first of $\mathtt{lg}(dm_1) \cdot \tilde{m}_2$. q.e.d.

2.66 Remark. Now one can switch to the distance vector representation of monomials completely for all computations. Since the direct shifting is not needed either, one has an efficient representation of the orbit under the shift action on a monomial.
The methods from the previous section can be directly applied and the correctness of those procedures is granted by 2.54. The benefit with this approach is that homogenization is not needed and the algorithm provides a counterpart to the usual non-commutative Buchberger algorithm, using commutative methods whenever possible, thereby increasing efficiency for steps like divisibility tests. Moreover, we can observe the following: Suppose that monomials of the free algebra are represented as words in an alphabet (say of the type string), then the divisibility of monomials is equivalent to subword searching. In the representation via distance vectors the monomials are represented by dense integer vectors with bounded entries and the divisibility of monomials can be solved via containment (as in Corollary 2.63)

2.5 Gebauer-Möller for the Letterplace Ring

Our goal now is to translate Gebauer-Möllers' criteria into the letterplace realm. Notably, in this criterion there is no distinction between graded and non-graded cases.

2.67 Theorem. Let P be the set of critical pairs. Suppose it contains a pair $\pi = (p_i, s \cdot p_k)$ for $p_i, p_k \in W \subset \mathbb{K}[\mathbf{X} \mid P]$ and $s \in \mathbb{N}$.

1. If there exist two pairs $\pi_1 = (p_i, s' \cdot p_j)$ and $\pi_2 = (p_j, s'' \cdot p_k)$, such that $\mathtt{lm}(s' \cdot p_j) | \mathtt{lcm}(p_i, s \cdot p_k)$, then the S-polynomial $s(\pi)$ of π will reduce to zero.

2. If there exists a pair $\pi_1 = (p_j, s \cdot p_k) \neq \pi$, such that $\mathtt{lcm}(p_j, s \cdot p_k)$ divides $\mathtt{lcm}(p_i, s \cdot p_k)$, then the S-polynomial $s(\pi)$ of π will reduce to zero.

Proof: Immediate consequence of 1.59. q.e.d.

2.68 Remark. Ad 1.: We have $s'' = s - s'$. This follows immediately from the non-commutative proof 1.59 and the form of the overlap. In the case, when the shifts are already known, commutative methods can be used to check the divisibility. For condition one this is especially easy, since from the concrete pair we check its shift is known.
Ad 2.: Since we assume that the shift of p_k is the same for π and π_1, the condition, that $\mathtt{cm}(\pi_1)$ divides $\mathtt{cm}(\pi)$ from the right, is always satisfied.

Although from a theoretical point of view the criteria do not differ much from the non-commutative case the version for the letterplace ring has some significant advantages. Since the shift is given by earlier computations in the Gröbner basis algorithm the divisibility check can be done using purely commutative methods or applying the methods given by the usage of distance vectors. In a later chapter we will see that this approach is indeed feasible.

2.6 Representation of Orderings over the Letterplace Ring

2.69 Definition. Assume we have $\mathbb{K}[\mathbf{X} \mid P]$ equipped with an ordering $\preceq$. Define a new ordering on $\mathbb{K}\langle\mathbf{X}\rangle$ by $m \leq n \Leftrightarrow \iota(m) \preceq \iota(n)$. We call $\leq$ the *ordering corresponding to* $\preceq$ or simply *corresponding ordering.*

2.70 Remark. Given an ordering on $\mathbb{K}\langle\mathbf{X}\rangle$ it is not as simple to define a related ordering on $\mathbb{K}[\mathbf{X} \mid P]$, since $\mathbb{K}[\mathbf{X} \mid P]$ has much more elements.
Robbiano proves in [Rob85] that every monomial ordering for each finitely generated polynomial ring originates from a matrix ordering. It is not clear that Robbiano's classification works in the general setting of letterplace rings because those are not finitely generated. However, if we add a degree bound d to $\mathbb{K}\langle\mathbf{X}\rangle$ we can consider the subring $L_d = \mathbb{K}[\mathbf{X} \mid \{1, \ldots, d\}]$, which is a finitely generated ring, and the theorem is applicable. The question arises if each ordering for $\mathbb{K}\langle\mathbf{X}\rangle$ can be viewed as corresponding to some ordering for $\mathbb{K}[\mathbf{X} \mid P]$, at least up to a certain degree.

For a given ordering $\leq$ on $\mathbb{K}\langle\mathbf{X}\rangle$ it is clear that one can order the monomials, spanning the vector space V correspondingly. If this is viewed as a preordering one can apply a method similar to the one in the first chapter (see 1.27)and get an ordering for L_d. However, there are more points to consider than just multiplicativity. For example we demand that $\preceq$ is shift invariant, so the preordering should allow $m \succeq s \cdot m \quad \forall s \in \mathbb{N}, s > 1, m \in [\mathbf{X} \mid P]$, as well as

$s \cdot m \preceq s \cdot n \quad \forall m, n \in [\mathbf{X} \mid P]$ with $m \preceq n$.
Moreover, on $\mathbb{K}\langle \mathbf{X} \rangle$ we have $x * x = x^2$, while on L_d we have $x(1) * x(1) = x(1)^2$, where $*$ denotes the standard ring multiplication. But what we need for multiplicativity is $x(1) \cdot_{lp} x(1) = x(1)x(2)$, where $\cdot_{lp}$ denotes the multiplication as in 2.34. So the question arises whether we always can achieve multiplicativity and whether the $\star$ multiplicativity is always satisfied as well. Note that those two properties are not connected to each other.
Indeed we only need to order *place-linear* monomials of $\mathbb{K}[\mathbf{X} \mid P]$ since those are the interesting ones for our computations. So the exponent vectors we need to consider are in $\{0,1\}^{nd}$.

Let us consider some examples first. The goal hereby is to find a matrix on the letterplace ring such that the corresponding ordering is something we desire. Later we will check out some other properties of those orderings.

2.71 Example. For each of these examples we will consider $\mathbb{K}\langle \mathbf{X} \rangle$ with n variables and the corresponding letterplace ring $\mathbb{K}[\mathbf{X} \mid P]$. Assume the variables of $\mathbb{K}[\mathbf{X} \mid P]$ are ordered in a natural way regarding the places, that is $x_1(1) > \ldots > x_n(1)$,
$x_1(2) > \ldots > x_n(2) > \ldots$.

1. We start by considering the identity matrix, so $\mathbb{K}[\mathbf{X} \mid P]$ is equipped with the lexicographical ordering. By restricting this ordering to the vector space V one easily sees that this corresponds to the left lexicographical ordering on $\mathbb{K}\langle \mathbf{X} \rangle$. Note that on $\mathbb{K}[\mathbf{X} \mid P]$ this respects the standard multiplication, but not the $\star$ multiplication, since on $\mathbb{K}\langle \mathbf{X} \rangle$ the left lexicographical ordering is not multiplicative.

2. Now consider $A = \begin{pmatrix} 1 & 1 & \cdots \\ Id & 0 & \end{pmatrix}$, where Id is an infinite identity matrix. This is easily identified as the graded lexicographical ordering on $\mathbb{K}[\mathbf{X} \mid P]$ as well as on $\mathbb{K}\langle \mathbf{X} \rangle$.

3. If we replace the first line in the matrix of the second example with an vector of (positive) integers we get a (positive) weighted ordering. However, not every choice holds a corresponding ordering for the free algebra.

   a) Assume $w \in \mathbb{N}^n$ and replace the first line by $w, w, w, \ldots$. Then this corresponds directly to the weighted ordering on the free algebra.

   b) For simplicity we take $n = 2$ and take $A = \begin{pmatrix} 1 & 2 & 3 \ldots \\ 1 & 0 & 0 \ldots \\ 0 & 1 & 0 \ldots \\ \vdots & \vdots & \vdots \end{pmatrix}$, which induces a shift-invariant weight ordering on the letterplace ring $\mathbb{K}[x_1, x_2 \mid \mathbb{N}]$. One can check that the corresponding ordering is in fact a multiplicative well-ordering, although the weighting might be a little strange. This is due to the fact that the difference in the weights scales consistently over the places.

c) Again we take $n = 2$, but this time we set $A = \begin{pmatrix} 1&2&2&1&1&\dots \\ 1&0&0&0&0&\dots \\ 0&1&0&0&0&\dots \\ \vdots&\vdots&\vdots& & & \end{pmatrix}$, which induces a weighted degree ordering on the letterplace ring $\mathbb{K}[x_1, x_2 \mid \mathbb{N}]$. Note that this ordering is not shift-invariant and therefore the corresponding ordering will not be multiplicative.

2.72 Example. • For this example we rearrange our variables in the following way: $x_1(1), \dots, x_n(1), x_n(2), \dots, x_1(2), x_1(3) \dots$. Again if we take the identity matrix we get a lexicographical ordering. However, if we now look upon the corresponding ordering it is no longer the lexicographical ordering, but a non-multiplicative ordering, which orders monomials depending on the position of the variables. By reordering the variables to the previous setting one gets another matrix $A' = \begin{pmatrix} I_n & 0 & 0 & \dots \\ 0 & I_n^{rev} & 0 & \dots \\ 0 & 0 & I_n & \dots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}$, where $I_n^{rev} = \begin{pmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix}$, representing the same ordering on $\mathbb{K}[\mathbf{X} \mid P]$.

- This time let us take $\mathbb{K}\langle\mathbf{X}\rangle$ together with the right lexicographical ordering and try to find a matrix for a corresponding ordering on $\mathbb{K}[\mathbf{X} \mid P]$. We fix a degree bound d. Note that $\mathbb{K}[\mathbf{X} \mid P]_d$ is a ring in nd variables. With a little effort one can show that there exists no matrix which induces a corresponding ordering.
  This can be done by solving a system of inequalities: For example take $d = 4$ and $\mathbb{K}\langle x, y\rangle$. We assume we have a matrix $A = (a_{i,j})_{1 \le i,j \le 4}$. Since we know that $x^2 > yx > x > xy > yy > y$ should hold we get (by translating those inequalities to the letterplace ring):

$$\begin{aligned}
a_{1,1} + a_{1,3} &\ge a_{1,2} + a_{1,3} \ge a_{1,1} \ge a_{1,1} + a_{1,4} \ge a_{1,2} + a_{1,4} \ge a_{1,2} \\
a_{2,1} + a_{2,3} &\ge a_{2,2} + a_{2,3} \ge a_{2,1} \ge a_{2,1} + a_{2,4} \ge a_{2,2} + a_{2,4} \ge a_{2,2} \\
a_{3,1} + a_{3,3} &\ge a_{3,2} + a_{3,3} \ge a_{3,1} \ge a_{3,1} + a_{3,4} \ge a_{3,2} + a_{3,4} \ge a_{3,2} \\
a_{4,1} + a_{4,3} &\ge a_{4,2} + a_{4,3} \ge a_{4,1} \ge a_{4,1} + a_{4,4} \ge a_{4,2} + a_{4,4} \ge a_{4,2}
\end{aligned}$$

  The third inequality already holds that $a_{1,4} = a_{2,4} = a_{3,4} = a_{4,4} = 0$, therefore we have a contradiction to the fact that A should be a full rank matrix.

  One can avoid this problem. Let us fix $d \in \mathbb{N}$ and define a map $\hat{\iota} : \langle\mathbf{X}\rangle_d \to [\mathbf{X} \mid P] : m \mapsto (d - \operatorname{tdeg}(m)) \cdot \iota(m)$. We will see later that there also holds a correspondence between all polynomials up to degree d and some vector space in $\mathbb{K}[\mathbf{X} \mid P]$, therefore the choice is reasonable. Choose $A = \begin{pmatrix} 0&0&\dots&0&I_n \\ 0&0&\dots&I_n&0 \\ \vdots&\vdots&\vdots&\vdots&\vdots \\ I_n&0&\dots&0&0 \end{pmatrix}$. Then it is easy to verify that $m \le n \iff \hat{\iota}(m) \le_A$

$\hat{\iota}(n)$ $\forall m, n \in \mathbb{K}\langle \mathbf{X} \rangle_d$. By reordering the variables of $\mathbb{K}[\mathbf{X} \mid P]_d$ one can see that A induces again a lexicographical ordering on $\mathbb{K}[\mathbf{X} \mid P]_d$.

2.73 Example (Elimination)**.** For these examples we consider $\mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$, that is we divide our set of variables in two subsets. We want to study elimination orderings for $\mathbf{X}$.

- The easiest way to eliminate all variables in $\mathbf{X}$ is to apply weights in the way that all variables in $\mathbf{X}$ have weight one and all variables in $\mathbf{Y}$ have weight zero, which is often done in the commutative case. Recall that this ordering while having the elimination property will not be multiplicative, as an example similar to the case of the lexicographical ordering shows. However, one can use a matrix for weighted orderings as in the example above to realize this ordering, since this is only a special case of a weighted ordering.

- Note that the left lexicographical ordering is also a (non-multiplicative) elimination ordering, but only for the first variable and if viewed as a special case of the first example. With the example above one can create another matrix inducing the lexicographical ordering by giving the first variable in each place weight one, thus changing the first row, moving each other row one down and deleting the last line.

- Let $d \in \mathbb{N}$ be a fixed degree bound. To realize the ordering *Elim* over $\mathbb{K}[\mathbf{X} \mid 1, \ldots, d]$ one can choose the matrix $A = \begin{pmatrix} I_n & I_n & \ldots & I_n & I_n \\ I_n & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & I_n & 0 \end{pmatrix}$ with $A \in \mathbb{K}^{nd \times nd}$.

All those examples motivate the following result.

2.74 Lemma. Suppose $\mathbb{K}\langle \mathbf{X} \rangle$ is equipped with a monomial ordering $\leq$ and a degree bound d is fixed. Moreover, suppose that the monomials of the vector space V are ordered accordingly. If this ordering can be extended to a monomial ordering $\preceq$ on $\mathbb{K}[\mathbf{X} \mid 1, \ldots, d]$ then there exists a matrix representation for this ordering and $\leq$ is the corresponding ordering of $\preceq$.

Proof: The existence of the matrix is a consequence of Robbiano's Theorem [Rob85] applied to $\mathbb{K}[\mathbf{X} \mid \underline{d}]$. Since we require that $\preceq$ orders the elements of V according to the ordering of the elements of $\mathbb{K}\langle \mathbf{X} \rangle$ the claim follows. q.e.d.

As the number of examples shows it is often possible to extend the given ordering to a monomial ordering on the letterplace ring, even if sometimes *block-wise* repositioning of the variables of $\mathbb{K}[\mathbf{X} \mid P]$ is required, as seen in example 2.72. However, it is unclear in which cases this procedure does not work, since most orderings can indeed be handled in this way.

There is another motivation for our studies of representation of orderings:
In SINGULAR, every ordering presented by a non-degenerate matrix can be realized. So in this regard realizing orderings over the letterplace ring as matrices becomes even more useful.

As a next step we study the orderings on the letterplace ring itself to see, which ones have desired properties and how those translate to the free algebra. We start by noticing that there are two kinds of multiplication we should consider.

2.75 Remark. If we view $\mathbb{K}[\mathbf{X} \mid P]$ as a polynomial ring we have the standard multiplication $*$. However, this means that $x(1) * x(1) = x(1)^2$, which does not correspond to a monomial in the free algebra. So we recall the definition of the $\star$ multiplication 2.46: For $m_1, m_2 \in \mathbb{K}[\mathbf{X} \mid P]$ we define $m_1 \star m_2 := m_1 * (\mathtt{pdeg}(m_1) \cdot m_2)$. We then have $x(1) \star x(1) = x(1) * x(2) = x(1)x(2)$ as desired.

So achieving multiplicativity for the standard multiplication alone will not be enough to ensure a monomial ordering on the free algebra. The notion of shift invariance comes to mind. However, if one does consider the (left) lexicographical ordering this shows that even then the corresponding ordering, namely the lexicographical, has nice properties, while $\leq_{\mathrm{llex}}$ is not multiplicative. So given a matrix ordering on $\mathbb{K}[\mathbf{X} \mid P]_d$, the question arises which properties the matrix must have to ensure a corresponding ordering to be a monomial ordering.

We introduce another property which we do require of our ordering.

2.76 Definition. An ordering is called *shift compatible* if

$$\mathtt{shift}(p) = \mathtt{shift}(\mathtt{lm}(p)) \quad \forall p \in \mathbb{K}[\mathbf{X} \mid P] \setminus \{0\}.$$

2.77 Remark. If we have a linear preordering on the variables of $\mathbb{K}\langle\mathbf{X}\rangle$ we can order the variables of $\mathbb{K}[\mathbf{X} \mid P]$ for the first place analogously. Requiring shift invariance this preordering can be extended to all variables of $\mathbb{K}[\mathbf{X} \mid P]$ uniquely. Shift compatibility however ensures that $x_i(j) > x_i(k)$ whenever $j < k$. Moreover, this adds the interesting property that any ordering will become an elimination ordering for the variables in place one. This is useful for the fact that we are only interested in elements of the vector space V.

2.78 Example. As we have seen the matrix $A = \left(\begin{smallmatrix} 1 & 1 & \cdots \\ Id & 1 & \\ & & 0 \end{smallmatrix}\right)$ corresponds to the graded lexicographical ordering on the free algebra as well as the same ordering on $\mathbb{K}[\mathbf{X} \mid P]$. However it is easily seen that it is not shift compatible as an ordering on $\mathbb{K}[\mathbf{X} \mid P]$, as the example $x(2)x(3)x(4) + x(1)$ shows. However, if we fix a degree bound d, set $E = (1, \ldots, 1) = 1^n$ and choose

$$A' = \begin{pmatrix} E & 0 & 0 & \ldots & 0 \\ 0 & E & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & E \\ I_{n-1} & 0 & 0 & \ldots & 0 \\ 0 & I_{n-1} & 0 & \ldots & 0 \\ 0 & 0 & \ldots & I_{n-1} & 0 \end{pmatrix},$$

then the corresponding ordering will still be the graded lexicographical ordering, while $\mathbb{K}[\mathbf{X} \mid P]$ is equipped with a shift invariant and compatible ordering, which is a consequence of the structure of the matrix. To see that the correspondence is correct note that the total degree is compared place-wise.

2.79 Remark. The examples of 2.78 shows that two different matrices may define the same ordering on $\mathbb{K}[\mathbf{X} \mid P]_d$, so one can ask if there is a sort of normal form for each ordering which should be chosen and which operation are allowed in order to simplify any given matrix. However, only a few operations are allowed if one does not want to change the ordering (namely adding upper rows to lower once and multiplying positive integers to rows) and none of them will transform A into A', which is due to the fact that viewed as orderings on $\mathbb{K}[\mathbf{X} \mid P]$ A induces a different ordering than A'.

Considering the matrix A' from above one can note that it has a special structure: If we take stripes of n columns the i-th stripe is the first stripe shifted i times downwards.

2.80 Definition. Take $v, v' \in K^n$ viewed as columns. Then v' is called *received from v by shifting i times downward* if $v'[1] = \ldots = v'[i] = 0$ and $v'[i+1] = v[1], \ldots v'[n] = v[n-i+1]$. A matrix A is said to contain *shifted stripes of length n* if for each $1 \neq i \in \underline{d}$, where nd is the number of columns of A, the columns $(i-1)n+1$ to in are the same as the first n columns shifted $i-1$ times downward.

2.81 Remark. Arranging columns into stripes of length n resembles to the fact that one can grade the vector space V' by places, that is $V' = V \oplus 1 \cdot V \oplus 2 \cdot V \oplus \ldots$, so one sorts the variables (and their order) also by places.
Since a matrix inducing an ordering has to be of full rank, no zero rows are allowed. So the first row of the first stripe will always be non-zero, because the first row of all other stripes will be zero. That implies that each ordering induced by a matrix containing shifted stripes will always eliminate the variables in the first place.

2.82 Lemma. If an ordering $\preceq$ on $\mathbb{K}[\mathbf{X} \mid P]$ is represented by a matrix containing stripes of length n then $\preceq$ is shift invariant and shift compatible.

Proof: The shift invariance is clear by the structure of the matrix.
For shift compatibility take $p \in \mathbb{K}[\mathbf{X} \mid P]$ and assume $\mathtt{shift}(p) \neq \mathtt{shift}(\mathtt{lm}(p))$ that is there is a monomial m in p such that $\mathtt{shift}(m) < \mathtt{shift}(lm(p))$. Therefore there is $x_i(j)$ contained in m such that $j < \mathtt{shift}(lm(p))$. This is a contradiction to the fact that orderings invoked by matrices containing shifted stripes are always eliminating variables in lower places. q.e.d.

2.83 Remark. The question arises whether every shift invariant and compatible ordering is representable by such a matrix. Obviously the best way to represent a shift compatible ordering is by choosing a matrix that contains shifted stripes,

because then one is able to describe the ordering on the infinitely generated letterplace ring with finite data, namely with the first stripe. It is easy to see that, with a fixed degree bound d, the first stripe will be a sparse $n \times nd$ matrix and all other stripes can be retrieved from the first one. So in which situations is one allowed to choose a matrix containing shifted stripes?

2.84 Proposition. Every shift invariant and shift compatible monomial ordering on $\mathbb{K}[\mathbf{X} \mid P]$, which does not eliminate any of the variables in $\mathbf{X}$, can be represented by a matrix containing shifted stripes of length n.

Proof: First we note that if the claim holds for $\mathbb{K}[\mathbf{X} \mid \underline{d}]$ with $d \in \mathbb{N}$ then it is also true for $\mathbb{K}[\mathbf{X} \mid P]$, since one can extend the matrix. So assume we have a shift invariant and shift compatible monomial ordering on $\mathbb{K}[\mathbf{X} \mid \underline{d}]$ for some $d \in \mathbb{N}$. Since we assume we have a monomial ordering we can present it by a matrix A, which contains positive entries. We divide it into $n \times n$ submatrices and refer to them by indices $A_{i,j}$ to differentiate from the entries $A[i, j]$.
Since $m < n$ implies $s \cdot m < s \cdot n \quad \forall m, n \in [\mathbf{X} \mid \underline{d}], s \in \mathbb{N}$ such that $s \cdot m, s \cdot n \in \mathbb{K}[\mathbf{X} \mid \underline{d}]$ we have that the matrix $A_{\star,j}$ formed by the first j columns of A must contain the same information as the matrix $(A_{\star,j'})_{s<j' \leq s+d'}$, where d' denotes the highest place occurring in m and n. For $s, s' \in \mathbb{N}$ such that $s < s'$ we have $x_i(s) > x_i(s')\ \forall i \in \underline{d}$ and therefore we can conclude that the stripes of columns must have length n.
Since A must have full rank and $x_i(s) > x_i(s')$ whenever $s < s'$ there exists $i \in \mathbb{N}$ with $1 \leq i \leq n$ such that $A[1, i] > 0$. Assume $A[1, ki] > 0$ with $ki \leq d$ and $1 < k \in \mathbb{N}$. Obviously we have $A[1, ki] < A[1, i]$. Because each submatrix of columns must contain the same information as before we get $A[1, ki] > 0\ \forall 1 < k \leq d$. If $A[1, i] < d$ this leads to a contradiction to $A[1, k'i] < A[1, ki]$ for $k' > k$, so assume $A[1, i] \geq d$. But then the total degree of $x_i(1)$ exceeds the degree bound, which either implies a elimination ordering for x_i or all the other variables are also equipped with a weight > 1. Because of the assumptions the latter case holds, so we can reduce the weights until the minimal weight equals 1, therefore achieving $A[1, i] < d$, reaching once more a contradiction. Therefore $A[1, ki] = 0\ \forall 1 \leq i \leq n, 1 < k \leq d$.
Iterating this step for submatrices we get the desired form for A. q.e.d.

2.85 Remark. In fact there always exists a good representation as long as we do not choose a elimination ordering. There are two problems we would like to answer: Can any given matrix inducing a shift invariant and compatible ordering be retrieved from a matrix containing shifted stripes and for which orderings on $\mathbb{K}\langle\mathbf{X}\rangle$ can we achieve shift invariance and compatibility? Both question are equally hard to answer.
While with the theorem above one can always choose a matrix containing stripes the relation between two matrices is in no way clear and the application of Robbiano's classification is not helpful either.

As for the second question it is easy to see that each ordering which is compatible with the total degree of a polynomial will be in fact shift compatible. However, weighted orderings as well as the left lexicographical ordering can be viewed as corresponding orderings to shift compatible once.

As stated before the ordering *Elim* is a monomial elimination ordering. However, by the choice of the matrix we made for an ordering on the letterplace ring it is not shift compatible. This is due to the fact that the elimination property divides the set of variables into two parts which are dealt with separately in some way. Say we have the set $\{X, Y\}$ as variables and we want to eliminate X with a fixed degree bound d as usual. We can achieve a matrix with stripes of length d if we order the variables by places first, that is

$$x_1(1), \ldots, x_1(d), x_2(1), \ldots, x_k(d), y_1(1), \ldots, y_{k'}(d).$$

However, the ordering will not be shift compatible, since the stripes are not of length n and the choice implies an ordering which considers variables first and does not prioritize the place.

As one can see finding a good representation for an ordering can be quite complicated. In practice however there are often good representations available, as the large amount of examples in this section shows.

2.7 Conclusion

The work done in [LL09] and [Sca12] showed that the letterplace approach is promising and should be investigated further. The implementations done to test the theoretical approach showed good results. However, they were never intended to be optimal.

In this work we showed that there is indeed a way to compute Gröbner bases of arbitrary ideals and that one does not have to rely on homogenization. We have also revealed that there is no direct correspondence between a non-graded ideal in the free algebra and some special kind of ideals in the letterplace ring. However, we can identify the free algebra in the letterplace ring by adding an additional structure, the $\star$-multiplication (see 2.46).

The new data structure introduced in this work, the so-called distance vectors, are not only a fascinating structure to apply the theoretical results, but also an excellent choice to represent monomials of the free algebra on the computer, therefore allowing an optimized and efficient implementation of the letterplace Gröbner basis algorithm.

The new insights we gained by studying representation matrices of orderings over the letterplace rings are of interest for implementations as well as from a

theoretical point of view. Since the computer algebra system SINGULAR allows to use any ordering presented by a matrix the results presented here are of practical value. The discussion which properties an ordering needs to be considered *good* may lead to a classification of orderings in a future work.

3 Gröbner Basics

The most common applications of Gröbner basis computations are sometimes called Gröbner basics. In this chapter we like to present those methods and state algorithms which can solve a variety of problems.

At the beginning we should discuss the notion of decidability. Most of the procedures we present need a Gröbner basis as input or, in some cases, a Gröbner basis must be computed during the procedure. As mentioned before Gröbner bases might contain infinitely many elements due to the lack of Noetherianity of $\mathbb{K}\langle\mathbf{X}\rangle$. In those cases the computations may not lead to a result, which is the reason some of the questions presented here are not decidable in general.

3.1 Truncated Gröbner Bases

While it is sometimes impossible or at least very hard to compute a complete Gröbner basis, sometimes necessary and valuable information can be retrieved from the knowledge of a part of a complete Gröbner basis. In this section we define what a *part of a Gröbner basis* is, following [Stu10] and try to gather first information from this part.

3.1 Definition. Let G be a set of polynomials such that $\operatorname{tdeg}(g) \leq q \; \forall g \in G$ and some $q \in \mathbb{N}$. In Algorithm 1.55 discard every obstruction with an S-polynomial of total degree greater than q. If the algorithm returns the set G_q, we call G_q a *truncated Gröbner basis of degree* q.
Let G be a Gröbner basis for $\langle G\rangle$ and $\tilde{G} \subset G$. We call $\tilde{G}$ a *partial Gröbner basis*, if it is already a Gröbner basis for the ideal $\tilde{I} := \langle\tilde{G}\rangle$.

Since 1.55 always computes a reduced Gröbner basis, a truncated Gröbner basis will also be reduced. Note that a truncated Gröbner basis does not necessarily need to be a subset of our reduced Gröbner basis. But since the algebra $\mathbb{K}\langle\mathbf{X}\rangle$ has only finitely many variables there are only finitely many monomials of total degree $\leq q$ (up to scaling), so the "truncated" version of the algorithm will terminate in any case.

It is clear, that $\langle G_q\rangle = \langle G\rangle$, since Algorithm 1.55 does not change the generated ideal. So we may use G_q to get to know more about the Gröbner basis we want to compute.

3.2 Lemma. Let $B \subseteq \mathbb{K}\langle \mathbf{X} \rangle$ and G_q be a truncated Gröbner basis of degree q of $\langle B \rangle$. If $\max\{\mathrm{tdeg}(g) \mid g \in G_q\} \leq \frac{q}{2}$ then G_q is a Gröbner basis of the ideal generated by B.

Proof: Define $m := \max\{\mathrm{tdeg}(g) \mid g \in G_q\}$. Since $\langle B \rangle = \langle G_q \rangle$ we only need to show: Every S-polynomial of obstructions of polynomials in G_q is of degree at most $2m-1$, which implies the claim.
Take $g_m \in G_q$ such that $\mathrm{tdeg}(g_m) = m$. Take an arbitrary $g_i \in G_q$, such that $(l, i, r; \lambda, m, \rho)$ is a left, right or central obstruction. Note that $\mathrm{tdeg}(g_i) \leq \mathrm{tdeg}(g_m) \quad \forall g_i \in B$, so all obstructions we need to consider are of the form $(l, i, r; \lambda, m, \rho)$. Because of 1.49 we may assume that $\mathtt{lm}(g_i)$ and $\mathtt{lm}(g_m)$ have overlap $b \neq 1$.

1. Assume $\mathtt{lm}(g_i) = ab$ and $\mathtt{lm}(g_m) = bc$ with $\mathrm{tdeg}(b) \geq 1$.
   Clearly $(1, i, c; a, m, 1)$ is an obstruction and the induced S-polynomial is of degree at most $2m-1$, since b is not a constant.
   Let $(1, i, r; \lambda, m, \rho)$ be a right obstruction. Since $\mathtt{lm}(g_i r) = \mathtt{lm}(\lambda g_m \rho) \Leftrightarrow ab\mathtt{lm}(r) = \mathtt{lm}(\lambda)bc\mathtt{lm}(\rho)$ we get $\mathtt{lm}(\lambda) = a$ and $\mathtt{lm}(r)$ and $c\mathtt{lm}(\rho)$ have overlap c. So $s(1, i, r; \lambda, m, \rho) = g_i c\tilde{r} - a g_m \tilde{\rho}$ for some $\tilde{r}, \tilde{\rho} \in \mathbb{K}\langle \mathbf{X} \rangle$, which is weak with respect to $G_q \cup \{s(1, i, c; a, m, 1)\}$ by the definition of weakness.
   Now let $(l, i, 1; \lambda, m, \rho)$ be a left obstruction.
   As before we get $s(l, i, 1; \lambda, m, \rho) = \tilde{l} g_i c - \tilde{\lambda} a g_m$, which is weak with respect to $G_q \cup \{s(1, i, c; a, m, 1)\}$.
   By assumption there will not be any central obstruction.

2. The case $g_i = ba$ and $g_m = cb$ is completely analogous to part 1.

3. Because the degree of g_m is maximal, the last case we have to study is $g_m = a g_i b$. But this would imply that g_m is weak with respect to $G_q \setminus \{g_m\}$ which is a contradiction to the assumption that G_q is a truncated Gröbner basis. q.e.d.

3.3 Corollary. If G_q is a truncated Gröbner basis, then $H := \{p \in G_q \mid \mathrm{tdeg}(p) \leq \lfloor \frac{q}{2} \rfloor\}$ is a partial Gröbner basis for $\langle G_q \rangle$.

Proof: Clear by 3.2. q.e.d.

Provided there exists a finite Gröbner basis, this leads to a way to compute the whole Gröbner basis starting with a truncated one, by iteratively increasing the degree bound.

3.4 Algorithm.

Input: A (finite) truncated Gröbner basis G_q for $I = \langle G_q \rangle$
Output: A reduced Gröbner basis for I

($\star$) $p := \max\{\mathrm{tdeg}(g) \mid g \in G_q\}$
Apply the truncated version of Algorithm 1.55 to G_q with degree bound $2p-1$ and call the result G_{2p-1}
if $p = \max\{\mathrm{tdeg}(g) \mid g \in G_{2p-1}\}$ **then**
return G_{2p-1}
else: go to ($\star$)
end if

3.5 Remark. It is obvious that 3.4 terminates, if there exists a finite Gröbner basis, and that it will return this Gröbner basis of I.
The proof of Lemma 3.2 states that if we construct an S-polynomial we will lose at least one degree to the overlap, since it is not trivial. This illustration shows us that our lemma includes only the worst case. In fact most of the time we will not have to double our q for the truncated Gröbner basis, as the following lemma states:

3.6 Lemma. Let $B \subseteq \mathbb{K}\langle \mathbf{X} \rangle$ and G_q be a truncated Gröbner basis of degree q of B. Take $g_1 \in G_q$ of degree m, and $g_2 \in G_q$ of maximal degree, say o, such that g_2 has a non-trivial and non-central overlap with g_1. Define $l := lcm(\mathtt{lm}(g_1), \mathtt{lm}(g_2))$, where lcm denotes the least common multiple, that is $lcm(\mathtt{lm}(g_1), \mathtt{lm}(g_2)) := \max_{\mathrm{tdeg}(b)} \{abc \in \langle \mathbf{X} \rangle \mid a, b, c \in \langle \mathbf{X} \rangle,\ abc = \mathtt{lm}(g_1)c = a\mathtt{lm}(g_2),\ \mathtt{lm}(g_1) \text{ and } \mathtt{lm}(g_2) \text{ have overlap } b\}$ and set $p := \mathrm{tdeg}(l)$. Then $m + 1 \leq p \leq m + o - 1$.

Proof: Assume $\mathtt{lm}(g_1) = ab$ and $\mathtt{lm}(g_2) = bc$ for some $a, b, c \in \langle \mathbf{X} \rangle$, which corresponds to a right obstruction. Since the overlap is non-trivial, none of the monomials a, b, c equal one, so they are all of positive degree. Therefore $l = abc$ is of degree $p = \mathrm{tdeg}(abc) = \mathrm{tdeg}(g_1) + \mathrm{tdeg}(c) \geq m + 1$ on the one hand and on the other $p = \mathrm{tdeg}(abc) = \mathrm{tdeg}(ab) + \mathrm{tdeg}(c) \leq \mathrm{tdeg}(ab) + \mathrm{tdeg}(bc) = m + o$.
By relabeling g_1 and g_2 we get the case of a left obstruction as above. q.e.d.

3.7 Proposition. Let $B \subseteq \mathbb{K}\langle \mathbf{X} \rangle$ and G_q be a truncated Gröbner basis of degree q of B. Take $g_1 \in G_q$ of degree m, and $g_2 \in G_q$ of maximal total degree, say o, such that g_2 has any non-trivial overlap with g_1. The overlap may have total degree p.
If we can write $g_1 = \mathtt{lm}(g_1) + \tilde{g_1}$, $\mathrm{tdeg}(\tilde{g_1}) = \tilde{m} \leq m$ and $g_2 = \mathtt{lm}(g_2) + \tilde{g_2}$, $\mathrm{tdeg}(\tilde{g_2}) = \tilde{o} \leq o$, then the total degree of the normal form of any S-polynomial of G_q is at most m', where $m' = \max\{\tilde{m}(o-p), \tilde{o}(m-p)\}$.

Proof: The only two obstructions we need to consider are $(1, 2, c; a, 1, 1)$ and $(c, 2, 1; 1, 1, a)$, as seen in the proof of Lemma 3.2. In the first case, we have

$$\mathrm{tdeg}(c) = \mathrm{tdeg}(g_1) - \mathrm{tdeg}(b) = m - p, \quad \mathrm{tdeg}(a) = \mathrm{tdeg}(g_2) - \mathrm{tdeg}(b) = o - p.$$

Since the leading terms of g_1 and g_2 cancel each other, we have

$$\mathrm{tdeg}((1,2,c;a,1,1)) \leq \max\{\tilde{m}(o-p), \tilde{o}(m-p)\}.$$

For the second case we get analogously:

$$\mathrm{tdeg}((c,2,1;1,1,a)) \leq \max\{\tilde{m}(o-p), \tilde{o}(m-p)\}.$$

q.e.d.

The bound given in Proposition 3.7 is again not strict: It determines the highest total degree p of all S-polynomials. Therefore, we have to compute a Gröbner basis at least up to degree p. But if all S-polynomials of total degree p reduce to zero the degree bound needed is in fact lower. However, 3.7 can be used to enhance Algorithm 3.4 in an obvious way:

3.8 Algorithm. Input: A truncated Gröbner basis G_q for $I = \langle G_q \rangle$
Output: A reduced Gröbner basis for I
($\star$) Set:

$$p := \max\{\mathrm{tdeg}(m) \mid m = \mathtt{lm}(S(g,\tilde{g})), (g,\tilde{g}) \in G_q \times G_q, \\ g \text{ and } \tilde{g} \text{ have non trivial overlap}\}$$

for $g \in \{\tilde{g} \in G_q \mid \mathrm{tdeg}(\tilde{g}) = p\}$ **do**

$$p_g := \max\{p + d_{\tilde{g}} - p_{g,\tilde{g}} \mid d_{\tilde{g}} = \mathrm{tdeg}(\tilde{g}), \\ p_{g,\tilde{g}} = \min\{o \mid g \text{ and } \tilde{g} \text{ have overlap of total degree } o\}, \\ \tilde{g} \in G_q\}$$

end for
Set $p = \max\{p_g \mid g \in \{\tilde{g} \in G_q \mid \mathrm{tdeg}(\tilde{g}) = p\}\}$
if $p \leq q$ **then**
  return G_q
  else: Apply the truncated version of Algorithm 1.55 to G_q with degree bound p and call the result G_p
  if $G_p = G_q$ **then**
    return G_p
    else: Set $G_q = G_p$ and go to ($\star$)
  end if
end if

3.9 Remark. Algorithm 3.8 will be of great use in the setup of the letterplace analogon. Here one always has a degree bound, at least in practice (cf. [LL09]).

So one always computes a truncated Gröbner basis. Therefore, the adaptive algorithm is the only way to get to a complete Gröbner basis.
It is in no way clear, whether this algorithm will terminate. In fact the question for termination is the question for finiteness of the Gröbner basis. In general, if the Gröbner basis is infinite, we do not have any possibility to determine that, whereas if the Gröbner basis is finite the Algorithm 3.8 will terminate.
However, there are some situations, when we can decide whether the Gröbner basis will be finite or not, as we will see in a later section.

3.2 Elimination

In 1.24 the notion of elimination ordering was introduced. Here we study applications of those orderings. This was also done by Nordbeck in [Nor98] and can also be found in [Xiu12].

We first introduce the notion of elimination ideal.

3.10 Definition. Assume we have a subset $\mathbf{Y} \subset \mathbf{X}$ and an ideal $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$. Set $\tilde{\mathbf{X}} = \mathbf{X} \setminus \mathbf{Y}$. Then the ideal $I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$ is called the *elimination ideal* of I with respect to $\mathbf{Y}$.

3.11 Lemma. Take an ideal $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ and a subset $\mathbf{Y} \subset \mathbf{X}$. Let $<$ be a elimination ordering for $\mathbf{Y}$ and set $\tilde{\mathbf{X}} = \mathbf{X} \setminus \mathbf{Y}$. Assume G is a Gröbner basis for I with respect to $<$. Then $G \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$ is a Gröbner basis for the elimination ideal $I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$.

Proof: Because of the elimination property we have $G \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle \subset I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$. Let $p \in I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle \setminus \{0\}$ be a polynomial. Since G is a Gröbner basis of I there are $\lambda, \rho \in \langle\mathbf{X}\rangle$ and $g \in G$ such that $\mathtt{lt}(p) = \lambda\mathtt{lt}(g)\rho$. Now since $p \in I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$ we have in particular $\mathtt{lt}(p) \in I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$ and therefore $\lambda, \mathtt{lt}(g), \rho \in I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$. Since we have chosen a elimination ordering this also implies $g \in I \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$ showing that $g \in G \cap \mathbb{K}\langle\tilde{\mathbf{X}}\rangle$. q.e.d.

One important application for elimination ideals is the computation of intersection of ideals.

3.12 Proposition. Consider two sets of polynomials G_1 and G_2 and assume $I_1 = \langle G_1\rangle$, $I_2 = \langle G_2\rangle \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$. Consider the free algebra $\mathbb{K}\langle y, \mathbf{X}\rangle$ in $n+1$ variables and set $C := \langle yx_i - x_iy \mid 1 \leq i \leq n\rangle$. Moreover, set $N := \{yf \mid f \in I_1\} \cup \{(1-y)g \mid g \in I_2\}$ consider the ideal $J = \langle N \cup C\rangle$. Then $I_1 \cap I_2 = J \cap \mathbb{K}\langle\mathbf{X}\rangle$.

Proof: Assume $p \in I_1 \cap I_2$. Then there are $g_{1,1}, \ldots, g_{k,1} \in G_1$ and $g_{1,2}, \ldots, g_{k',2} \in G_2$ such that $p = \sum_{i=1}^{k} l_{i,1}g_{i,1}r_{i,1} = \sum_{i=1}^{k'} l_{i,2}g_{i,2}r_{i,2}$ for some $l_{i,1}, l_{i,2}, r_{i,1}, r_{i,2} \in \mathbb{K}\langle\mathbf{X}\rangle$.

Now we can write $p = yp + (1-y)p = \sum_{i=1}^{k} yl_{i,1}g_{i,1}r_{i,1} + \sum_{i=1}^{k'}(1-y)l_{i,2}g_{i,2}r_{i,2} =$

$\sum_{i=1}^{k} l_{i,1} y g_{i,1} r_{i,1} + \sum_{i=1}^{k'} l_{i,2}(1-y) g_{i,2} r_{i,2} + p_C$, with $p_C \in C$. Obviously $\sum_{i=1}^{k} l_{i,1} y g_{i,1} r_{i,1} + \sum_{i=1}^{k'} l_{i,2}(1-y) g_{i,2} r_{i,2}$ shows that $p \in J \cap \mathbb{K}\langle \mathbf{X} \rangle$.

Now assume $p \in J \cap \mathbb{K}\langle \mathbf{X} \rangle$ that is $p = \sum_{i=1}^{k} l_{i,1} y g_{i,1} r_{i,1} + \sum_{i=1}^{k'} l_{i,2}(1-y) g_{i,2} r_{i,2} + p_C$ for some $g_{i,1} \in G_1, g_{i,2} \in G_2, l_{i,1}, l_{i,2}, r_{i,1}, r_{i,2} \in \mathbb{K}\langle y, \mathbf{X} \rangle$ and $p_C \in C$. Now since $p \in \mathbb{K}\langle \mathbf{X} \rangle$ the representation is independent of the choice of y, so we can substitute $y \mapsto 1$ and get $p = \sum_{i=1}^{k} l'_{i,1} g_{i,1} r'_{i,1} \in I$ with $l'_{i,1} = l_{i,1}(0, \mathbf{X}), r'_{i,1} = r_{i,1}(0, \mathbf{X}) \in \mathbb{K}\langle \mathbf{X} \rangle$. On the other hand if we set $y \mapsto 0$ we get $p = \sum_{i=1}^{k'} l'_{i,2} g_{i,2} r'_{i,2} \in J$, where $l'_{i,2} = l_{i,2}(0, \mathbf{X}), r'_{i,2} = r_{i,2}(0, \mathbf{X}) \in \mathbb{K}\langle \mathbf{X} \rangle$, showing that $p \in I_1 \cap I_2$. q.e.d.

As a result we get the following algorithm to compute intersection of two ideals.

3.13 Algorithm.
Input: $G_1,\ G_2$, two generating sets for ideals I_1 and I_2
Output: G, a Gröbner basis for $I_1 \cap I_2$
Consider $\mathbb{K}\langle y, \mathbf{X} \rangle$ and choose an elimination ordering for y.
Compute a Gröbner basis of $\{yf, (1-y)g, yx_i - x_i y \mid 1 \leq i \leq n, f \in I_1, g \in I_2\}$ and call it $\tilde{G}$.
return $G = \tilde{G} \cap \mathbb{K}\langle \mathbf{X} \rangle$

3.14 Remark. While in general the termination of this algorithm is not guaranteed unless a degree bound is added, the correctness is given by Proposition 3.12. Note that this algorithm can be generalized to the case of the intersection of s ideals $I_1, \ldots, I_s,\ s \in \mathbb{N}$ generated by the sets G_i. Then one needs to introduce $s-1$ new variables $\{y_1, \ldots, y_{s-1}\}$ and computes a Gröbner basis of $(\bigcup_{i=1}^{s-1} \{y_i g_{i_j} \mid g_{i_j} \in G_i\} \cup \{(1 - y_1 - \ldots - y_{s-1}) g_{s_j} \mid g_{s_j} \in G_s\}) \cup C$, where C denotes the set of all commutators between x_i and y_j.

As an application of this algorithm we study homomorphisms of algebras. More precisely we want to compute the kernel of such a homomorphism. We set $Y = \{y_1, \ldots, y_m\}$.

3.15 Proposition. Assume we have two finitely presented algebras $A = \mathbb{K}\langle \mathbf{Y} \rangle / J$ and $B = \mathbb{K}\langle \mathbf{X} \rangle / I$ and an algebra homomorphism

$$\varphi :\ A \to B :\ [y_i] \mapsto [g_i],\ i = 1, \ldots, m,$$

for some $g_i \in \mathbb{K}\langle \mathbf{X} \rangle$. Set $D := \langle y_1 - g_1, \ldots, y_m - g_m \rangle \trianglelefteq \mathbb{K}\langle \mathbf{X}, \mathbf{Y} \rangle$. Then we have $\ker(\varphi) = ((D + I) \cap \mathbb{K}\langle \mathbf{Y} \rangle) + J$.

Proof: Take $p \in \ker(\varphi) \subseteq \mathbb{K}\langle \mathbf{Y}\rangle/J$ and set $\phi(p) = q \in I \trianglelefteq \mathbb{K}\langle \mathbf{X}\rangle$. Then we have $q = p(g_1, \ldots, g_m)$. By using $y_i = (y_i - g_i) + g_i \ \forall 1 \leq i \leq m$ we can write $p(y_1, \ldots, y_m) = \tilde{p} + p(g_1, \ldots, g_m)$ for some $\tilde{p} \in D$. Now since $q \in I$ we have $p \in D + I \trianglelefteq \mathbb{K}\langle \mathbf{X}, \mathbf{Y}\rangle$ and since $p \in \mathbb{K}\langle \mathbf{Y}\rangle$ we have $p \in D + I \cap \mathbb{K}\langle \mathbf{Y}\rangle$, which implies $p + J \in D + I \cap \mathbb{K}\langle \mathbf{Y}\rangle + J$.
Now assume $p \in \mathbb{K}\langle \mathbf{Y}\rangle$ such that $p + J \in ((D + I) \cap \mathbb{K}\langle \mathbf{Y}\rangle) + J$. By definition we get $p = \sum_{i=1}^{m} l_i(y_{j_i} - g_{j_i})r_i + p_I + J$ for some $l_i, r_i \in \mathbb{K}\langle \mathbf{X}, \mathbf{Y}\rangle, p_I \in I$. Now $p(g_1, \ldots, g_m) = p_I \in I$ showing that $p + J \in \ker(\varphi)$. q.e.d.

3.16 Remark. This proposition can be applied as follows: Suppose we have $I = \langle G_I\rangle$ and $J = \langle G_J\rangle$. Set $H = \{y_1 - g_1, \ldots, y_m - g_m\} \cup G_I$ and choose an elimination ordering for $\mathbf{X}$. Now compute a Gröbner basis $\tilde{G}$ of H and set $G = \tilde{G} \cap \mathbb{K}\langle \mathbf{Y}\rangle$. Since G generates $(D+I) \cap \mathbb{K}\langle \mathbf{Y}\rangle$ by 3.11 we have $\ker(\varphi) = \langle G \cup G_J\rangle$.

As a consequence we are able to introduce another useful application.

3.17 Corollary. Say we have an elimination ordering for $\mathbf{X}$ on $\mathbb{K}\langle \mathbf{X}, \mathbf{Y}\rangle$. In the setup of 3.15 we have $[f] \in \mathtt{Im}(\varphi)$ if and only if $\mathtt{NF}(f, D + I) \in \mathbb{K}\langle \mathbf{Y}\rangle$.

Proof: Take $f \in \mathbb{K}\langle \mathbf{X}\rangle$ such that $[f] \in \mathtt{Im}(\varphi)$ that is there is $p \in \mathbb{K}\langle \mathbf{Y}\rangle/J$ such that $\varphi(p) = [f]$ that is $p(g_1, \ldots, g_m) + I = f + I$. We rewrite $g_i = y_i - (y_i - g_i)$ and get $p(g_1, \ldots, g_m) = p(y_1, \ldots, y_m) + \tilde{p}$ with $\tilde{p} \in D$ and therefore $\mathtt{NF}(f, D+I) = \mathtt{NF}(p, D + I)$, since $\mathtt{NF}(\tilde{p}, D + I) = 0$. Now since we have chosen a elimination ordering for $\mathbf{X}$and $p \in \mathbb{K}\langle \mathbf{Y}\rangle$ we also have $\mathtt{NF}(p, D + I) \in \mathbb{K}\langle \mathbf{Y}\rangle$ showing that $\mathtt{NF}(f, D + I) \in \mathbb{K}\langle \mathbf{Y}\rangle$.
Now take $f \in \mathbb{K}\langle \mathbf{X}\rangle$ such that $\mathtt{NF}(f, D+I) \in \mathbb{K}\langle \mathbf{Y}\rangle$. Then $f - \mathtt{NF}(f, D+I) \in D+I$ by the properties of normalforms. This implies a representation $f - \mathtt{NF}(f, D+I) = \sum_{i=1}^{m} l_i(y_{j_i} - g_{j_i})r_i + p_I$ with $l_i, r_i \in \mathbb{K}\langle \mathbf{X}, \mathbf{Y}\rangle, p_I \in I$. Therefore $\varphi(f - \mathtt{NF}(f, D+I)) \in I$ which implies $f + I = \varphi(\mathtt{NF}(f, D + I))$ that is $f + I \in \mathtt{Im}(\varphi)$. q.e.d.

3.18 Corollary. In the setup of 3.16 we have φ is surjective if and only if $\tilde{G}$ contains elements $x_i - h_i$ where $h_i \in \mathbb{K}\langle \mathbf{Y}\rangle \ \forall 1 \leq i \leq n$.

Proof: Consequence of 3.17. q.e.d.

Proposition 3.15 can be used to find a practical way to decide whether or not an element of $\mathbb{K}\langle \mathbf{X}\rangle/I$ is *algebraic*.

3.19 Definition. Consider a finitely presented algebra A and take an element $g \in A$. We call g *algebraic* if there is $0 \neq p \in \mathbb{K}[y]$ such that $p(g) = 0$. We call $\min_{\mathrm{tdeg}(p)} \{p \in \mathbb{K}[y] \mid p(g) = 0, \mathtt{lc}(p) = 1\}$ the *minimal polynomial* of g.

3.20 Lemma. Consider the algebra homomorphism $\varphi : \mathbb{K}[y] \to \mathbb{K}\langle \mathbf{X}\rangle/I : y \mapsto [g]$. We have $[g]$ is algebraic if and only if $\ker(\varphi) \neq \{0\}$. Moreover $\ker(\varphi)$ is generated by the minimal polynomial of $[g]$.

Proof: If $[g]$ is algebraic the exists $p \in \mathbb{K}[y]$ such that $p([g]) = [0]$ and therefore $p \in \ker(\varphi)$. On the other hand we have $p([g]) = [0]\ \forall p \in \ker(\varphi)$ which proves the first claim.
Since $\mathbb{K}[y]$ is a principal ideal domain $\ker(\varphi)$ is generated by one element p and we have for all elements in $\mathrm{tdeg}(p) \leq \mathrm{tdeg}(\tilde{p}) \quad \forall \tilde{p} \in \ker(\varphi)$. If we choose p to be normalized the second statement follows. q.e.d.

The proof shows that the minimum of the set $\{p \in \mathbb{K}[y] \mid p(g) = 0, \mathtt{lc}(p) = 1\}$ in Definition 3.19 exists and that it is unique.

Another important application for these methods is the *generalized word problem*. Given a set of generators $\mathbf{X}$ and a finitely presented monoid $M = \langle \mathbf{X} \mid R \rangle$, where R is a set of relations, we want to decide whether or not a given $m \in M$ is contained in a submonoid $S = \langle s_1, \ldots, s_r \rangle \subseteq M$. In general this problem is not decidable. However, under the assumption that each Gröbner basis is finite we can state a method which solves the problem.

3.21 Lemma. Let $M = \langle \mathbf{X} \mid R \rangle$ be a finitely presented monoid and take $S = \langle s_1, \ldots, s_r \rangle \subseteq M$. Say $\mathbb{K}M \cong \mathbb{K}\langle \mathbf{X} \rangle / I$ that is $I = \langle \{r_1 - r_2 \mid (r_1, r_2) \in R\} \rangle$ and take $m \in \langle \mathbf{X} \rangle$ and denote by $\overline{m}$ the corresponding element in M. Then $\overline{m} \in S$ if and only if $[m - 1] \in \mathbb{K}\langle s_1 - 1, \ldots, s_r - 1 \rangle \subseteq \mathbb{K}\langle \mathbf{X} \rangle / I$.

Proof: If we identify $\mathbb{K}M$ with its monoid ring $\mathbb{K}\langle \mathbf{X} \rangle / I$ it is obvious that S corresponds to the subalgebra $\mathbb{K}\langle s_1 - 1, \ldots, s_r - 1 \rangle$. q.e.d.

3.22 Remark. In the setup of 3.21 we consider the homomorphism of algebras $\varphi : \mathbb{K}\langle \mathbf{X} \rangle / I \to \mathbb{K}\langle \mathbf{X} \rangle / I : [x_i] \mapsto [s_i - 1]$. If $[m - 1]$ is in $\mathtt{Im}(\varphi)$ then $\overline{m}$ is contained in S, which solves the problem.
Note that we can generalize this to the setup of arbitrary subalgebras, thereby solving the analogous *subalgebra membership problem* in the case that the Gröbner basis is finite.

3.3 Syzygies

In this section we define the bi-module of syzygies for a Gröbner basis of an ideal $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$ and present a way to compute it. We are motivated by [KB07], where an algorithm to compute syzygies of elements of a free two-sided module over $\mathbb{K}\langle \mathbf{X} \rangle$ was presented and we like to show how the letterplace setup can be used as an easy way to implement this method.

We start with the definition of syzygies.

3.23 Definition. Assume we have a two-sided ideal $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$ given by a (finite) generating set $G = \{g_1, \ldots, g_s\}$ and denote by F_s the free two-sided $\mathbb{K}\langle \mathbf{X} \rangle$-module generated by $\{e_1, \ldots, e_s\}$. The *(two-sided) syzygy module* of G is defined as the kernel of the homomorphism of bimodules $\lambda : F_s \to \mathbb{K}\langle \mathbf{X} \rangle : e_i \mapsto g_i$. We will denote it by $\mathtt{Syz}(G)$.

3.24 Remark. Another way to define a syzygy is by using the relation $\sum_{i=1}^{s}\sum_{j} l_{i,j}g_i r_{i,j} = 0$. It is essential that we distinguish the elements which are multiplied from the right and those which are multiplied from the left, so when we say $\mathtt{Syz}(G)$ is a two-sided $\mathbb{K}\langle\mathbf{X}\rangle$-module we view it as an ($\mathbb{K}\langle\mathbf{X}\rangle$-$\mathbb{K}\langle\mathbf{X}\rangle^{opp}$)-bimodule (cf. 1.8).

Note that this definition can be extended for tuples of vectors of the free $\mathbb{K}\langle\mathbf{X}\rangle$-module F_r, but for our purpose we restrict ourself to the case $r = 1$.
The computation of a syzygy-module is based on the following theoretical layout.

3.25 Proposition. Denote by F_{s+1} the free $\mathbb{K}\langle\mathbf{X}\rangle$-module generated by $\{e_1, \ldots, e_{s+1}\}$. Take a subset $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}\langle\mathbf{X}\rangle$ and set $U = \langle g_1 \cdot e_1 - e_2, g_2 \cdot e_1 - e_3, \ldots, g_s \cdot e_1 - e_{s+1}\rangle \subset F_{s+1}$. Then we have $U \cap \langle e_2, \ldots, e_{s+1}\rangle \cong \mathtt{Syz}(G)$.

Proof: We set $\hat{F}_{r+s} = \langle e_{r+1}, \ldots, e_{r+s}\rangle$, $\overline{g}_i = g_i \cdot e_1$ and consider the homomorphism $\Psi : \hat{F}_{1+s} \to F_s : e_{1+i} \mapsto e_i$. The restriction ψ of Ψ to $U \cap \langle e_2, \ldots, e_{s+1}\rangle$ is then an injective homomorphism to F_s. So we need to show that $\mathtt{Im}(\psi) = \mathtt{Syz}(G)$. Let $s = \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}e_i r_{i,j} \in \mathtt{Syz}(G)$, where $c_{i,j} \in \mathbb{K}, l_{i,j}, r_{i,j} \in \langle\mathbf{X}\rangle$. Then $\hat{s} = \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}e_{1+i}r_{i,j} = \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}\overline{g}_i r_{i,j} + \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}(e_{1+i} - \overline{g}_i)r_{i,j}$ is an element in $U \cap \hat{F}_{1+s}$ and obviously we have $\phi(\hat{s}) = s$. On the other hand take $\hat{s} = \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}e_{1+i}r_{i,j} \in U \cap \hat{F}_{1+s}$. Then $\lambda(\phi(\hat{s})) = \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}\overline{g}_i r_{i,j} = \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}(\overline{g}_i - e_{1+i})r_{i,j} + \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}e_{1+i}r_{i,j} \in U$.

Now since $\lambda(\phi(\hat{s})) = \sum_{i=1}^{s}\sum_{j} c_{i,j}l_{i,j}\overline{g}_i r_{i,j}$ is a representation of $\lambda(\phi(\hat{s}))$ without the generators $\{e_2, \ldots, e_{s+1}\}$ this implies $\lambda(\phi(\hat{s})) = 0$, since $U = \langle g_1 \cdot e_1 - e_2, g_2 \cdot e_1 - e_3, \ldots, g_s \cdot e_1 - e_{s+1}\rangle$, so $\phi(\hat{s}) \in \mathtt{Syz}(G)$. q.e.d.

With this result we are able to formulate a procedure to compute the syzygies of G. Again we set $\hat{F}_{r+s} = \langle e_{r+1}, \ldots, e_{r+s}\rangle$.

3.26 Algorithm.
Input: $G := \{g_1, \ldots, g_s\} \subset \mathbb{K}\langle\mathbf{X}\rangle$
Output: $\tilde{G}$, a Gröbner basis for the two-sided syzygy module $\mathtt{Syz}(G)$
Define $\varphi : \hat{F}_{1+s} \to F_s : e_{i+1} \mapsto e_i \; \forall 1 \leq i \leq s$
Set $\overline{g}_i := g_i \cdot e_1 \; \forall 1 \leq i \leq s$ and choose an ordering on F_{s+1} which eliminates the first component
Compute a Gröbner basis for $\{\overline{g}_1 - e_2, \overline{g}_2 - e_3, \ldots, \overline{g}_s - e_{s+1}\}$ and call it U
Compute $\hat{U} = U \cap \hat{F}_{1+s}$
return $\varphi(\hat{U})$

If $\mathtt{Syz}(G)$ has a finite Gröbner basis this algorithm terminates and returns a Gröbner basis for the two-sided syzygy module $\mathtt{Syz}(G)$.

Proof: By 3.25 we know that $\varphi(\langle \hat{U} \rangle) \cong \mathtt{Syz}(G)$. That $\hat{U}$ forms a Gröbner basis is a consequence of 3.11. q.e.d.

3.27 Remark. With the methods of the previous section we can now compute the syzygy module. Note that this algorithm is similar to the commutative algorithm (see for example [GP08] or [Lev05]). There one can visualize the method using matrices. Assume we have $I = \langle g_1, \ldots, g_s \rangle \trianglelefteq \mathbb{K}[\mathbf{X}]$ and set

$$F := \begin{pmatrix} g_1 & g_2 & \cdots & g_s \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

We put the result of the Gröbner basis computation of the matrix F with respect of a position-over-term monomial module ordering in the matrix M, sorting the columns in such a way, that the elements which are zero in their first component are moved to the left. Then

$$M = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & h_1 & \cdots & h_k \\ & \mathbf{S} & & & \mathbf{T} & \end{array}\right),$$

where we have

- The set $\{h_1, \ldots, h_k\}$ is a Gröbner basis for I.
- The columns of $\mathbf{S}$ generate $\mathtt{Syz}(\{g_1, \ldots, g_s\})$.
- The matrix $\mathbf{T}$ is a transformation matrix between $G = \{g_1, \ldots, g_s\}$ and $H = \{h_1, \ldots, h_k\}$.

We refer to [Lev05] for details about this procedure.

Notably, this approach does not work for two-sided ideals and bimodules. One way to apply this algorithm in the commutative case is to introduce new variables $\{e_2, \ldots, e_{s+1}\}$ and *idealize* the module structure. Those variables satisfy the condition $e_i e_j = 0 \; \forall 1 \leq i, j \leq s+1$ and those are added to the relations as well.

Because of the bimodule structure the non-commutative case is more complicated. Usually one wants to add commutators for the new variables as well, but since one needs to distinguish left from right multiplication the position of the e_i inside a monomial is essential. Note that the letterplace ring is again a natural choice for the computations, because the notion of *position* of a variable is part of the structure.

Without adding relations however our computations may hold elements we have no use for, namely those polynomials containing words in more than one e_i. So one has to discard those superfluous elements.

We now state an algorithm which uses idealization.

3.28 Algorithm.
Input: $G = \{g_1, \ldots, g_s\}$, a set of polynomials
Output: $\tilde{H}$, a set of polynomials in $\mathbb{K}[\mathbf{X}, e_2, \ldots, e_{s+1} \mid P]$
Set $\tilde{G} = \{g_1 - e_2, \ldots, g_s - e_{s+1}\}$ and choose an elimination ordering for $\{e_i \mid i = 2, \ldots, s+1\}$
Compute H, a Gröbner basis of $\tilde{G}$
Take $\tilde{H} = \{p \in H \mid p = \sum_i a_i m_i,\ \forall i\ \exists!\ k :\ e_k | m_i\} \subseteq H$
return $\tilde{H}$

3.29 Lemma. Assume we have a set of polynomials $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}\langle\mathbf{X}\rangle$ and a Gröbner basis S for $\mathtt{Syz}(G) \subset F_s$. Define a ring homomorphism

$$\sigma : \mathbb{K}\langle\mathbf{X}, e_2, \ldots, e_{s+1}\rangle \to \mathbb{K}\langle\mathbf{X}\rangle : x_i \mapsto x_i, e_i \mapsto g_{i-1}$$

and a map

$$\varsigma : \mathtt{Syz}(G) \to \mathbb{K}\langle\mathbf{X}, e_2, \ldots, e_{s+1}\rangle :$$
$$\sum_j (l_{j,1}\epsilon_{j,1}r_{j,1}, \ldots, l_{j,s}\epsilon_{j,s}r_{j,s}) \mapsto \sum_j \sum_{i=1}^{s} l_{j,i} e_{i+1} r_{j,i}.$$

Then:

- The set H in Algorithm 3.28 is a Gröbner basis for $\ker(\sigma)$.
- We have $\varsigma(S) = \tilde{H}$, where $\tilde{H}$ is the set returned by Algorithm 3.28.

Proof:

- It is clear that H is indeed a Gröbner basis. By 3.25 we have $\langle H\rangle = \ker(\sigma)$.
- Consequence of the correctness of 3.26. q.e.d.

3.30 Remark. It is worth to mention that the letterplace structure can be used very efficiently. Since all the variables are equipped with places we get a natural order of left and right coefficients, namely if e_i appears in place k, all variables up to place k are left coefficients, all with place greater than k are right coefficients.

One application for the computation of syzygies is the so called *conjugator search problem*. In [KB07] there is an algorithm proposed which is able to solve the

problem. We present this method here as well and apply it in the next chapter to some examples.

For now we will assume that G is a finitely presented group, that is we have a finite alphabet $\mathbf{X}$ and an equivalence relation $\sim_W$ which is the normal closure of finitely many relations $w_1 \sim w_1', \ldots, w_t \sim w_t'$ such that $G \equiv \langle \mathbf{X} \rangle / \sim_W$. Moreover, we assume we have a monomial ordering on $\langle \mathbf{X} \rangle$ such that $w_i > w_i' \ \forall 1 \leq i \leq t$ and that the *word rewriting system* $w_i \to w_i'$ is terminating and confluent that is the normal form of words with respect to $\sim_W$ can be computed.

The conjugator search problem can be stated as follows: Given a group G and two elements $g, h \in G$ which are *conjugated* to each other, find a conjugator or in other words find $a \in G$ such that $ag = ha$.

The assumptions we made are necessary to solve the *word problem* in G and therefore we have ensured that our computations will terminate. The method we present can be applied to a more general setup, however it is not guaranteed that the computation will finish.

3.31 Remark. In order to present the group G we choose the group ring $\mathbb{K}G$ as introduced in 1.16. Therefore we choose the ideal $I = \langle w_1 - w_1', \ldots, w_t - w_t' \rangle$. Then we have $\mathbb{K}G \cong \mathbb{K}\langle \mathbf{X} \rangle / I$. To guarantee the correctness of our computations we require a Gröbner basis of I. Since the set $W = \{w_1 - w_1', \ldots, w_t - w_t'\}$ contains only binomials the Gröbner basis will also contain only binomials and without loss of generality we will assume that W already forms a Gröbner basis.

3.32 Algorithm ([KB07])**.**

Input: $g, h \in G$, where G is a group given by generators $\mathbf{X} = \{x_1, \ldots, x_n\}$ and relations $\{w_1 - w_1', \ldots, w_t - w_t'\}$

Output: FALSE, if g and h are not conjugated or
$a \in G$ such that $ag = ha$ otherwise.

Take $\mathbb{K}\langle x_1, \ldots, x_n, e_1, \ldots, e_6 \rangle$

Choose an ordering $\prec$ such that for any $t_1, t_1', t_2, t_2' \in \langle \mathbf{X} \rangle$:

$$t_1 e_i t_1' \succ t_2 e_j t_2' \Leftrightarrow \quad \begin{array}{l} i < j \text{ or} \\ i = j \text{ and } t_1' > t_2' \text{ or} \\ i = j \text{ and } t_1' = t_2' \text{ and } t_1 > t_2. \end{array}$$

Set $U = \{e_1 g - e_3, e_1 h - e_4, e_2 - e_3 - e_5, e_2 + e_4 + e_6, e_1(w_1 - w_1'), \ldots, e_1(w_t - w_t'), e_2(w_1 - w_1'), \ldots, e_2(w_t - w_t'), x_1 e_1 - e_1 x_1, \ldots, x_n e_1 - e_1 x_n, x_1 e_2 - e_2 x_1, \ldots, x_n e_2 - e_2 x_n\}$ and compute a Gröbner basis $\tilde{U}$ for U.

If there is an element of the form te_5 in $\tilde{U}$ **return:** t

else **return:** FALSE

3.33 Remark. If the ideal I in Remark 3.31 has a finite Gröbner basis then Algorithm 3.32 solves the conjugator search problem in G. Note that the ordering $\prec$ is an elimination ordering for $\{e_1, e_2, e_3, e_4\}$. For details we refer to [KB07].

Assume g and h are conjugated elements of a group G. It is easy to see that the solutions of the conjugator search problem correspond to syzygies of $(g, h) \in \mathbb{K}\langle\mathbf{X}\rangle^2$ of the form $ae_1 - e_2a$, where (e_1, e_2) denotes the standard basis of the free two-sided $\mathbb{K}G$-module. Since we are only able to compute syzygies of elements of $\mathbb{K}\langle\mathbf{X}\rangle$-modules and not $\mathbb{K}\langle\mathbf{X}\rangle/I$-modules one needs to add extra relations, which explains the complicated structure of the set U.

3.4 Factor Algebras

For a given ideal I we can consider the *factor algebra* $\mathbb{K}\langle\mathbf{X}\rangle/I := \{f + I \mid f \in \mathbb{K}\langle\mathbf{X}\rangle\}$, which is again a $\mathbb{K}$-algebra via $[f]\cdot[g] = [fg]$ and $[f]+[g] = [f+g] \quad f, g \in \mathbb{K}\langle\mathbf{X}\rangle$, where $[f] = f + I$. We will drop the brackets and identify $[f] \equiv \mathtt{NF}(f, I)$, whenever it is possible.

Our first goal here is to find a $\mathbb{K}$-basis which is suitable for our needs.

3.34 Lemma. Let G be a reduced Gröbner basis with respect to a monomial ordering $<$. Then the set of all irreducible monomials with respect to G forms a $\mathbb{K}$-basis of $\mathbb{K}\langle\mathbf{X}\rangle/\langle G\rangle$ and it is called *the* (monomial) basis of $\mathbb{K}\langle\mathbf{X}\rangle/\langle G\rangle$. In particular the monomial basis of $\mathbb{K}\langle\mathbf{X}\rangle/\langle G\rangle$ is also a $\mathbb{K}$-basis of $\mathbb{K}\langle\mathbf{X}\rangle/\mathtt{L}(\langle G\rangle)$ and we have $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathtt{L}(I)) = \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/I)$.

3.35 Remark. This statement is part of the famous Diamond Lemma [Ber78]. In order to compute a $\mathbb{K}$-basis for a factor algebra given by a Gröbner basis one needs to check all monomials for irreducibility. A detailed analysis including a better way to store a $\mathbb{K}$-basis by using so-called *mistletoes* was done in [Stu10]. For our purpose here we only need to know that there is an effective way to compute and use the monomial basis for $\mathbb{K}\langle\mathbf{X}\rangle/I$ provided one has a Gröbner basis for I.

It is worth noting that if only a truncated Gröbner basis for I is known the resulting set of monomials might contain superfluous elements which only form a *fake* basis for $\mathbb{K}\langle\mathbf{X}\rangle/I$ [Stu10].

3.4.1 Dimension computations

Before one starts with the computation of the monomial basis the question arises if it will be finite. In other words: is $\dim_{\mathbb{K}}(A) < \infty$? Therefore one builds up the *Ufnarovskij graph*.

Note that a word w over an alphabet $\mathbf{X}$ does not need to have finite length, while a monomial is of finite length by definition. However, keep in mind that we want to apply the results to monomials in the free algebra.

Let G be a set of words over the alphabet $\mathbf{X}$. We call a word w *standard* with respect to G if there is no $g \in G$ which is contained in w as a subword. For a finite word w this implies that w is normal with respect to G.

3.36 Definition. Given an alphabet $\mathbf{X}$ and a set of finite words G, we can define the *Ufnarovskij graph* G_U. Its vertex set V consists of all standard words $w \in \mathbf{X}^{l_G} = \{m \in \mathbf{X} \mid m = x_{i_1} \cdots x_{i_{l_G}}\}$, where $l_G := -1 + \max_{m \in G} \mathtt{lg}(m)$. For each $v, w \in V$ there is a directed edge (v, w) if and only if there exists $a, b \in \mathbf{X}$ such that $va = bw$ and $G \nmid va$.

The graph is named after Victor Ufnarovskij, who introduced it in his work [Ufn89] and discussed it further in [Ufn95].

3.37 Remark.
1. There is a one-to-one correspondence between paths of length l in G_U and standard words of length $l + l_G$. This implies that each infinite standard word corresponds to an infinite path in G_U, which must contain a cycle, because G_U has a finite vertex set due to the finiteness of $\mathbf{X}$ and G. Therefore we have $\dim_{\mathbb{K}}(\mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle) = \infty$ if and only if G_U contains a cycle.

2. If there exists an infinite word that is standard with respect to G, then either it is cyclic or it gives rise to a cyclic infinite word that is also standard with respect to G.

3.38 Lemma. If there exists an infinite word $w' \in \mathbf{X}$ that is standard with respect to G, then there also exists a cyclic infinite word $w \in \mathbf{X}$ that is standard with respect to G such that

$$\forall r, s \geq 1 : \; w[1 \ldots s] \leq w[r \ldots r + s - 1], \tag{3.1}$$

where $w[p \ldots q]$ is the subword of w obtained by removing the first up to the $(p-1)$-th and the $(q+1)$-th up to the last letter.

Proof: We will use $u \trianglelefteq v$ to denote that u is a prefix of v, respectively $u \triangleleft v$, if it is a proper prefix. Further we denote with u^t the word consisting of the concatenation of t copies of the word u.
Let $w' \in \mathbf{X}$ be infinite and standard with respect to G. Then w' gives rise to a cyclic infinite word $w'' = v'^{\infty}$, where $v' \in \mathbf{X}^p$ for some finite $p > 0$. Assume that v is the lexicographically smallest shift of v'. Then there is a $u \trianglelefteq v'$ such that $v'^{\infty} = uv^{\infty}$. Now define $w := v^{\infty}$ and the claim follows. q.e.d.

3.39 Remark. The lemma states that in order to find an infinite word, it suffices to use only words satisfying (3.1). So we will proceed as follows: For a given

Gröbner basis G we build up the Ufnarovskij graph. If $\mathbb{K}\langle\mathbf{X}\rangle/\langle G\rangle$ has infinite $\mathbb{K}$-dimension, the graph will contain a cycle; if it is finite, the graph will be a tree.
Note that the Ufnarovskij graph is only defined for finite Gröbner bases, since in an infinite one has no upper degree bound.

Again we refer to [Stu10] for more details as well as an effective algorithm to decide whether or not $\dim_{\mathbb{K}}(A) < \infty$ holds. Again one can also use a truncated Gröbner basis as input for the algorithm. If it returns that the $\mathbb{K}$-dimension is in fact finite than this will also be true for the case of a complete Gröbner basis. This relates to the fact that the *fake* dimension as introduced in [Stu10] is an upper bound for the $\mathbb{K}$-dimension.

In many cases algebras of interest do not possess a finite $\mathbb{K}$-basis. To have a measurement of how fast an algebra *grows* one introduces the so-called Gel'fand-Kirillov dimension.

To understand the basic concept we first define the Hilbert series of an algebra.

3.40 Definition. Consider a finitely generated graded algebra $A = \bigoplus_{d\in\mathbb{N}} A_d$. We call the formal series $\sum_{d\in\mathbb{N}_0} \dim_{\mathbb{K}}(A_d)t^d \in K[t]$ the *Hilbert series* of A. The *Hilbert function* of A is defined as $H(A) : \mathbb{N}_0 \to \mathbb{N}_0 : d \mapsto \dim_{\mathbb{K}}(A_d)$.
If A is generated by the elements in A_1 then $H(A) = \frac{P(t)}{(1-t)^\delta}$ for some $\delta > 0$ and $P(t)$ a polynomial with coefficients in $\mathbb{N}_0$. If there is a polynomial $P(A) \in \mathbb{K}[t]$ which is equal to $H(A)$ we call it the *Hilbert polynomial*.

In [Stu10] a straightforward way to compute the Hilbert series is presented. Here we need the notion to understand the concept of growth of an algebra which is related to the growth of the Hilbert function.

3.41 Definition. Let A be a finitely generated $\mathbb{K}$-algebra. Then there exists a $\mathbb{K}$-subspace $V \subset A$ such that A is generated by V as a $\mathbb{K}$-algebra. V induces a *standard finite dimensional filtration* $\{A_i | i \in \mathbb{Z}\}$ on A by setting $A_i := \{0\}$ for $i < 0$, $A_0 := V^0 := \mathbb{K}$ and $A_i := \sum_{j=1}^{i} V^j$ for $i > 0$, where $V^j = \langle\{\prod_{k=1}^{j} v_k \mid v_k \in V\}\rangle$.

- Consider the function $f(n) = \dim_{\mathbb{K}}(\sum_{i=0}^{n} V^i)$. We say A has *polynomial growth of degree* d if there is a polynomial $p \in \mathbb{R}[x]$ with $\operatorname{tdeg}(p) = d$ such that $f(n) \leq p(n)$ for $n \gg 0$. If there is a real number $\epsilon > 0$ such that $f(n) \geq \epsilon^n$ for $n \gg 0$ we say A has *exponential growth*.
- The *Gel'fand-Kirillov dimension* is defined as

$$\mathtt{dim}_{\mathtt{GK}}(A) := \limsup_{i\to\infty} \log_i(\dim_{\mathbb{K}}(A_i)).$$

3.42 Remark. Note that we have $\mathtt{dim}_{\mathtt{GK}}(A) = \limsup_{i\to\infty} \frac{\log(f(n))}{\log(n)}$ as an alternative way to define the Gel'fand-Kirillov dimension. Therefore we have that if A has polynomial growth of degree d then $\mathtt{dim}_{\mathtt{GK}}(A) = d$ and if A has exponential growth then $\mathtt{dim}_{\mathtt{GK}}(A) = \infty$. It is important to note that the Gel'fand-Kirillov dimension does not depend on the choice of the filtration. For details we refer to [MR87].

In [Ufn95] Victor Ufnarovskij introduces a method to measure the growth of an algebra. Therefore we introduce the graph of normal words.

3.43 Definition. Consider an alphabet $\mathbf{X}$ and a set of monomials $G \subset \langle \mathbf{X} \rangle$. Define a set V as the union of all elements of $\mathbf{X}$ and the set $\bigcup_{g\in G} \mathtt{suff}(g)$ where $\mathtt{suff}(g)$ is the set of all proper suffices of g. Moreover, define $E := \{(u,v) \in V \times V \mid \nexists g \in G : \ g|uv, \ \forall w \in V : \ w \trianglelefteq uv \Rightarrow w \trianglelefteq u\}$. Then the graph G_N defined by (V, E) is called the *graph of normal words*.

The following theorem was proven in [Ufn95] and lays down the connection between the graph of normal words and the growth of an algebra.

3.44 Theorem. Given an alphabet $\mathbf{X}$ and a finite set of interreduced monomials $G \subset \langle \mathbf{X} \rangle$, let G_N be the graph of normal words. If vertices are considered to be paths of length 0, then there is a bijection between paths in G_N and (non-empty) normal words with respect to G.

Proof: Since G is an interreduced set of monomials the edges of G_N consist of normal words. For an arbitrary normal word n we use induction over the length l. If $l = 1$ then $n = x_i$ and therefore we have a path of length 0. Now assume $l > 1$. Since each proper subword of n is again normal of length $< l$ and are therefore represented as paths in G_N. Now if there is a vertex $v \in G_N$ such that $n = vw$, then w is normal and therefore represented by a path p. Since vw is normal and the set is interreduced there is a path between v and a prefix of w and we can extend p by chosing v as a new starting point. If there is no prefix of n occuring as eh vertex we choose the suffix of n of length $l-1$ which is again normal and call the corresponding path $\tilde{p}$ and the starting vertex v and we assume the first variable in n is x_i. Then, with the same argument as before, we can extend p by choosing x_i as new starting point. q.e.d.

3.45 Corollary. Consider $\mathbb{K}\langle \mathbf{X} \rangle$ equipped with a monomial ordering and say G is a finite and reduced Gröbner basis for $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$. Construct the graph of normal words G_N with respect to $\mathtt{L}(G)$. Then there is a bijection between paths in G_N and the $\mathbb{K}$-basis of $\mathbb{K}\langle \mathbf{X} \rangle / I$.

Proof: The set $\mathtt{L}(G)$ is a finite set of interreduced monomial, therefore 3.44 is applicable. q.e.d.

In order to state an algorithm which can evaluate the graph of normal words we need to introduce the concept of an incidence matrix.

3.46 Definition. Given a finite graph $\Gamma = (V, E)$ with $V = \{v_1, \ldots, v_n\}$ we define a matrix $T \in \mathbb{N}_0^{n \times n}$ as follows: We set $T(i, j) = k$ if there are exactly k edges going from v_i to v_j. We call T the *incidence matrix* of Γ.

Since for the graph of normal words there is at most one edge leading from one vertex to another we have $T \in \{0, 1\}^{n \times n}$.
The following algorithm was introduced in [Ufn95] and it computes the growth of an algebra presented as a factor of $\mathbb{K}\langle \mathbf{X} \rangle$.
We denote by $T(i, *)$ the ith row of T and by $T(*, i)$ the ith column.

3.47 Algorithm.
Input: G, a Gröbner basis for $I \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$
Output: $d \in \mathbb{N}_0$ or ∞, the Gel'fand-Kirillov dimension of $\mathbb{K}\langle \mathbf{X} \rangle / I$
Construct the graph of normal words G_N with respect to $\mathtt{L}(G)$.
Let T be the incidence matrix of G_N and set $D = 0 \in \mathbb{N}^{1 \times n}$.
†
if $T = 0$ **then**
return $\max\{D(i) \mid 1 \leq 1 \leq n\}$
end if
for $i = 0, \ldots, n$ **do**
if $T(i, i) \neq 0$ **then**
if $T(i, i) > 1$ or $(T(i, i) = 1$ and $D(i) > 0)$ **then**
return ∞
end if
if $T(i, i) = 1$ and $D(i) = 0$ **then**
$T(i, i) := 0$, $D(i) := 1$, go to †
end if
end if
end for
for $i = 0, \ldots, n$ **do**
if $T(i, *) \neq 0$ and $T^2(i, *) = 0$ **then**
$T(i, *) := 0$, $D(i) := D(i) + \max\limits_{j, T(i,j) \neq 0}(D(j))$, go to †
end if
end for
Find a cycle $v_{i_1} \to \ldots \to v_{i_k} \to v_{i_1}$.
$A(i_1, *) := \sum\limits_{j=i_1}^{i_k} A(j, *)$, $A(i_j, *) := 0 \quad \forall 2 \leq j \leq n$
$A(*, i_1) := \sum\limits_{j=i_1}^{i_k} A(*, j)$, $A(*, i_j) := 0 \quad \forall 2 \leq j \leq n$
$A(i_j, i_j) := A(i_j, i_j) - k + 1$
$D(i_l) := \sum\limits_{j=i_1}^{i_k} A(*, j) \quad \forall 1 \leq l \leq n$
Go to †

3.48 Remark. To see that the algorithm is correct we have to note that $T(i,*) \neq 0$ and $T^2(i,*) = 0$ implies that v_i is the-last-but-one vertex on a path (see [Ufn95]). In each step a loop is removed, a cycle is removed or a vertex is replaced by a terminal one. Because the number of vertices is finite this guarantees termination of the algorithm.

To find a cycle one can apply a classical deep-first search algorithm (see for example [CSRL01]). There are some obvious improvements to the algorithm, for example it is more effective to look for a cycle and handling along the way the-last-but-one vertices.

While the Gel'fand-Kirillov dimension is a good tool to measure the growth of an algebra it is not the only important notion of dimension. The notion of global dimension holds interesting informations about the algebra as well.

3.49 Definition. Let R be a ring and M and R (left) module.

- A *projective resolution* of M is an infinite exact sequence of modules $\ldots \to P_n \to \ldots P_2 \to P_2 \to P_1 \to M \to 0$ such that all P_i are projective modules. A resolution is called *finite*, if there exists $N \in \mathbb{N}$ such that $P_k = 0 \; \forall k > N$ and $P_N \neq 0$. The number N is called the *length* of the resolution.
- The *projective dimension* $\dim_{\mathtt{proj}}(M)$ of M is the minimal length among all finite projective resolutions of M.
- The *(left) global dimension* is defined to be the supremum of the set of all projective dimensions of all (left) R-modules. We write $\mathtt{gldim}(R)$.

3.50 Remark. One can also define the right global dimension by considering right modules of R. Note that those dimension usually do not coincide. However, if R is a Noetherian ring, both of these dimensions turn out to be equal to the *weak global dimension*, whose definition is left-right symmetric (cf. [MR87]).

Before trying to compute the global dimension for ideals in $\mathbb{K}\langle \mathbf{X} \rangle$ we give two examples why it is of interest.

3.51 Theorem (Anick)**.** Let $G \subset \langle \mathbf{X} \rangle$ be an interreduced subset with $G \cap \mathbf{X} = \emptyset$. Suppose $\mathtt{gldim}(\mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle) = m \in \mathbb{N}$. If $\mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle$ does not contain a free subalgebra of two generators, then the following statements hold:

1. $\mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle$ is finitely presented, that is, $\langle G \rangle$ is finitely generated.
2. $\mathtt{dim}_{\mathtt{GK}}(\mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle) = m$.
3. The Hilbert series of $\mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle$ is of the form $H_{\mathbb{K}\langle \mathbf{X} \rangle / \langle G \rangle}(t) = \prod_{i=1}^{m} (1 - t^{e_i})^{-1}$, where $e_i \in \mathbb{N} \; \forall 1 \leq i \leq m$.

Proof: [Ani86]

3.52 Theorem (Gatea-Ivanova)**.** Let $I \trianglelefteq \mathbb{K}\langle \mathbf{X}\rangle$ be a $\mathbb{N}$-graded ideal and suppose that $\mathtt{L}(I) \cap \mathbf{X} = \emptyset$, where $\mathtt{L}(I)$ is chosen with respect to a $\mathbb{N}$-graded monomial ordering. Moreover, assume that $\mathtt{dim}_{\mathtt{GK}}(\mathbb{K}\langle \mathbf{X}\rangle/\mathtt{L}(I)) = m \in \mathbb{N}$ and $\mathtt{gldim}(\mathbb{K}\langle \mathbf{X}\rangle/\mathtt{L}(I)) < \infty$. Then the following statements hold:

1. $\mathtt{gldim}(\mathbb{K}\langle \mathbf{X}\rangle/\mathtt{L}(I)) = \mathtt{gldim}(\mathbb{K}\langle \mathbf{X}\rangle/I) = m$.
2. The ideal I has a finite Gröbner basis.
3. The Hilbert series of $\mathbb{K}\langle \mathbf{X}\rangle/\langle G\rangle$ is of the form $H_{\mathbb{K}\langle \mathbf{X}\rangle/\langle G\rangle}(t) = \prod_{i=1}^{m}(1-t^{e_i})^{-1}$, where $e_i \in \mathbb{N}\ \forall 1 \leq i \leq m$.

Proof: [GI89]

We want to state an algorithm which can give an upper bound for the global dimension. Therefore we define yet another graph introduced by Victor Ufnarovskij.

3.53 Definition. Given an alphabet $\mathbf{X}$ and a set of interreduced monomials $G \subset \langle \mathbf{X}\rangle$. Denote by $\mathtt{suff}(g)$ the set of all proper suffices of the monomial g. We define the *graph of n-chains* $\Gamma_n(G) := (V, E)$, where $V := \{1\} \cup \mathbf{X} \cup \{\mathtt{suff}(g) \mid g \in G\}$ is the set of vertices and and we have $(u, v) \in E \subset V \times V$ if either $u = 1$ and $v = x_i$ for some $1 \leq i \leq n$ or $u, v \in V \setminus \{1\}$ and there exists $w = x_{i_1} \cdots x_{i_m} \in \langle \mathbf{X}\rangle$ such that $uv = w \in G$ or $uv = sw$ with $s \in \langle \mathbf{X}\rangle$ such that $sx_{i_1} \cdots x_{i_{m-1}} \in \langle \mathbf{X}\rangle \setminus \langle G\rangle$. An *d-chain* is a monomial $v \in \langle \mathbf{X}\rangle$ such that there is a route $1 \to v_1 \to \ldots \to v_d \to v_{d+1}$ of length $d+1$ and $v = v_1 \cdots v_d v_{d+1}$.

3.54 Theorem (Anick)**.** Say we have a Gröbner basis G for an ideal I. Then $\mathtt{gldim}(\mathbb{K}\langle \mathbf{X}\rangle/\langle G\rangle) \leq d$ if and only if $\Gamma_n(G)$ contains no d-chains.

Proof: [Ani85]

In [Ufn95] a way is presented to build up the graph of n-chains. Since we are only interested in d-chains it suffices to build about the connected component of the vertex 1. To do this there is an algorithm, which is used in [Kro03] to compute the Hilbert series. However, it can be used to compute the longest d-chain occurring in the graph. To show an alternative way to [Stu10] to compute the Hilbert series we state the algorithm in its original form. Since we already know that $\{1\}, \mathbf{X} \subset V$ and $(1, x_i) \in E\ \forall 1 \leq i \leq n$ we can start the graph in the generators. We define the length of a vertex to be the length of the monomial seen as a word of the alphabet $\mathbf{X}$. We write $\mathtt{lg}(w)$ for the length of the word w. For a list L and $l \in L$ we denote by $\mathtt{pos}(l, L)$ the position of l in L.

3.55 Algorithm.

Input: $G \subset \langle \mathbf{X} \rangle$, a finite set of interreduced monomials

Output: (V, E), the subgraph of $\Gamma_n(G)$ only containing the connected component of the vertex 1, L, a set containing the length of each vertex

```
Set V = X, E = ∅ and L[i] = 1 for 1 ≤ i ≤ n
for v ∈ V and g ∈ G do
  Determine S := {r ∈ ⟨X⟩ | g is a suffix of vr}
  if S ≠ ∅ then
    Set s = min_< {r ∈ S}
    Let s' be the largest proper prefix of s
    if vs' is normal with respect to G then
      if s ∉ V † then
        V = V, s; L = L, lg(s);
        Add pos(s, V) to E[pos(v, V)]
      end if
    end if
  end if
end for
return (V, E), L
```

3.56 Remark. Although elements can be added to V, the algorithm will terminate, since G is finite and there are only finitely many different suffices of elements of G. The reason to keep track of the length of vertices is to construct the Hilbert series, which can be expressed as $H := \sum_i (\text{number of } n\text{-chains of length } i)t^i$. This approach was used in [Kro03]. If one is only interested in computing an upper bound for the global dimension one does not need to keep track of those lengths.

To utilize Theorem 3.54 one can either build up the graph and search for the longest d-chain, or check for the longest d-chain while the graph is constructed. Obviously the latter one is slightly more efficient, especially in the case that that there is no upper bound. In that case $\Gamma_n(G)$ will contain a cycle, which implies that the condition $s \notin V$ (see †) will not be satisfied and we can immediately return ∞ at that point.

3.4.2 Left ideals in factor algebras

We assume we have $\mathbb{K}\langle \mathbf{X} \rangle$ equipped with an arbitrary monomial ordering and we take an ideal I with a finite Gröbner basis G. If we consider an ideal J of the algebra $A := \mathbb{K}\langle \mathbf{X} \rangle / I$ we know that there is a one-to-one correspondence to all ideals $J' \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$ which contain I as a subset. If J is a two-sided ideal generated by a set E it is easy to see that that in order to get a Gröbner basis for J we only need to compute a Gröbner basis of the set $E \cup G$ and then reduce the result with respect to the Gröbner basis G. However, if we consider J as a left ideal

things get a little more complicated. Recall that we have $J = {}_A\langle E\rangle := \{\sum c_i e_i \mid c_i \in A, e_i \in E\}$. We identify elements of A with their normal forms modulo I.

Note that the whole theory can also be done for right ideals. This was for example done in [Xiu12].

3.57 Definition. Let $J \trianglelefteq \mathbb{K}\langle \mathbf{X}\rangle$ be a left ideal containing the two sided ideal I, and let $G \subset J$ be a set of non-zero polynomials, normal with respect to I. We call G a (left) Gröbner basis of the ideal $J/I \trianglelefteq \mathbb{K}\langle \mathbf{X}\rangle/I$ if for every polynomial $p \in J/I$ there exists a polynomial $g \in G$ such that $\mathtt{lt}(g)$ is a suffix of $\mathtt{lt}(p)$. In other words $\mathtt{lt}(g)$ is a right divisor of $\mathtt{lt}(p)$, that is $\mathtt{lt}(p) = m\mathtt{lt}(g)$ for some $m \in \langle \mathbf{X}\rangle/I$.

Our first goal is to give an algorithm which allows us to do reduction with respect to J/I.

3.58 Algorithm. Input: $p \in \mathbb{K}\langle \mathbf{X}\rangle$, $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}\langle \mathbf{X}\rangle \setminus \{0\}$, g_i normal with respect to $I = \langle G\rangle \trianglelefteq \mathbb{K}\langle \mathbf{X}\rangle$
Output: $(v, q_1, \ldots, q_s) \in \mathbb{K}\langle \mathbf{X}\rangle^{s+1}$
Set $q_1 = \ldots = q_s = 0$ and $v = \mathtt{NF}_I(p)$.
while $\exists j \in \underline{s} : \mathtt{lt}(v) \equiv m\mathtt{lt}(g_j)$ for some $m \in \langle \mathbf{X}\rangle$ **do**
$q_j = q_j + \frac{\mathtt{lc}(v)}{\mathtt{lc}(g_j)}m$
$v = v - \frac{\mathtt{lc}(v)}{\mathtt{lc}(g_j)}m$
end while
return $(v, q_1, \ldots, q_s)$

3.59 Theorem. Algorithm 3.58 returns a tuple $(v, q_1, \ldots, q_s)$ such that

- $p - (\sum_{j_1}^{s} q_j g_j + v) \in I$.
- The polynomial v is in normal form with respect to I.
- For all $j \in \{1, \ldots, s\}$, q_j is in normal form with respect to I. If $q_j \neq 0$ for some $j \in \{1, \ldots, s\}$, then $\mathtt{lt}(p) \geq \mathtt{lt}(q_j g_j)$.
- If $v \neq 0$, then $\mathtt{lt}(p) \geq \mathtt{lt}(v)$ and there is no $j \in \{1, \ldots, s\}$ such that $\mathtt{lt}(g_j)$ is a suffix of $\mathtt{lt}(v)$.

Proof: To see that Algorithm 3.58 terminates we note that in each step the leading term of v strictly decreases. Since we have chosen a monomial ordering the procedure will stop after finitely many steps.
Since we have $q_j g_j + v = (q_j + \frac{\mathtt{lc}(v)}{\mathtt{lc}(g_j)}m)g_j + (v - \frac{\mathtt{lc}(v)}{\mathtt{lc}(g_j)}mg_j)$ in each step we get $p - (\sum_{j_1}^{s} q_j g_j + v) \in I$. Since v is set to be normal with respect to I we also get that $v - \frac{\mathtt{lc}(v)}{\mathtt{lc}(g_j)}m$ is normal with respect to I, therefore the second statement is

true. Since $\mathtt{lt}(v) = m\mathtt{lt}(g_j)$ is normal we also have that m must be a normal monomial, showing that each q_j contains only normal monomials and therefore is itself normal with respect to I. The latter statement of item (3) is a consequence of the fact that we have chosen a monomial ordering. The last statement is clear by the construction of v in the algorithm. q.e.d.

Note that Algorithm 3.58 only reduces the leading term of p. For a complete reduction we have to iterate over all terms of p after the leading term is completely reduced, that is restart the procedure with $p - \mathtt{lt}(p)$.

3.60 Definition. The polynomial v obtained in Algorithm 3.58 is called a *left normal form* of p. If we iterate the procedure for all terms we get the *reduced left normal form* or simply *the* left normal form, which we denote by $\mathtt{lNF}(p)$.

3.61 Proposition. Let $J \subseteq \mathbb{K}\langle \mathbf{X}\rangle$ be a left ideal containing I and let $G \subset J$ be a set of polynomials in normal form with respect to I. The following conditions are equivalent:

- The set G is a Gröbner basis of $J/I \trianglelefteq \mathbb{K}\langle \mathbf{X}\rangle/I$.
- Every normal polynomial $p \in J/I$ has a representation $p = \sum_{j=1}^{s} q_j g_j + h$ with $q_i \in \mathbb{K}\langle \mathbf{X}\rangle \setminus \{0\}, h \in I$ such that $\mathtt{lt}(p) \geq \mathtt{lt}(q_i g_i) \quad \forall i \in \{1, \ldots, s\}$ and $\mathtt{lt}(p) > \mathtt{lt}(h)$.
- A polynomial $p \in \mathbb{K}\langle \mathbf{X}\rangle$ satisfies $p \in J$ if and only if $\mathtt{lNF}(p) = 0$.

Proof: The equivalence of the first two items is clear by definition of left Gröbner basis, while the latter equivalence is a consequence of Theorem 3.59. q.e.d.

3.62 Remark. Taking a generating set E for J/I and a Gröbner basis G_I for I, each polynomial $p \in J/I$ can be represented as $p = \sum_{j=1}^{s} q_j e_j + \sum_i c_i l_i g_i r_i$, where $e_k \in E, q_k \in \mathbb{K}\langle \mathbf{X}\rangle \setminus \{0\}, c_k \in \mathbb{K}, g_k \in G_I, l_k, r_k \in \langle \mathbf{X}\rangle$. It is easy to see that this representation is not necessarily a representation like 3.61 (2), since there might be an index j such that $\mathtt{lt}(q_j)\mathtt{lt}(e_j) \geq \mathtt{lt}(p)$ or $l_j\mathtt{lt}(g_j)r_j \geq \mathtt{lt}(p)$. There are three cases in which these terms may occur:

1. There exist $j, j' \in \{1, \ldots, s\}, j \neq j'$ such that $\mathtt{lt}(q_j)\mathtt{lt}(e_j) \equiv \mathtt{lt}(q_{j'})\mathtt{lt}(g_{j'}) > \mathtt{lt}(p)$, that is e_j and $g_{j'}$ have an left overlap.
2. There exist $j, j' \in \{1, \ldots, s\}, j \neq j'$ such that $l_j\mathtt{lt}(g_j)r_j \equiv l'_{j'}\mathtt{lt}(g_{j'})r_{j'} > \mathtt{lt}(p)$, that is g_j and $g_{j'}$ have an overlap.
3. There $j \in \{1, \ldots, s\}, j' \in \mathbb{N}$ such that $\mathtt{lt}(q_j)\mathtt{lt}(e_j) \equiv l_{j'}\mathtt{lt}(g_{j'})r_{j'}$. Since e_j is normal with respect to I and G_I is a Gröbner basis this implies there is $w \in \langle \mathbf{X}\rangle \setminus \{1\}$ such that $\mathtt{lt}(q_j)\mathtt{lt}(e_j) \equiv \mathtt{lt}(g_{j'})w$.

Since G_I is a Gröbner basis for I one does not need to consider the second case, because one can simply use the Gröbner representation given by G_I.

3.63 Proposition. Let $G \subset J$ be a set of polynomials in normal form with respect to I and let $J/I \trianglelefteq \mathbb{K}\langle \mathbf{X}\rangle/I$ be the left ideal generated by G. Suppose we have a finite Gröbner basis G_I for I. Define two sets as follows:

$$O_G = \{\frac{1}{\mathtt{lc}(g)}g - \frac{1}{\mathtt{lc}(g')}wg' \mid g, g' \in G, g \neq g', w \in \langle \mathbf{X}\rangle, \mathtt{lt}(g) \equiv w\mathtt{lt}(g')\}$$

and

$$O_{GG_I} = \{\frac{1}{\mathtt{lc}(g)}wg - \frac{1}{\mathtt{lc}(g')}g'r' \mid g \in G, g' \in G_I, w, r' \in \langle \mathbf{X}\rangle, w\mathtt{lt}(g) \equiv \mathtt{lt}(g')r'\}.$$

Then G is a left Gröbner basis of J/I if and only if $lnf(p) = 0$ for all $p \in O_G \cup O_{GG_I}$.

Proof: If G is a left Gröbner basis then by 3.61 we have $lnf(p) = 0$ for any $p \in J/I$. Suppose now $lnf(p) = 0$ for all $p \in O_G \cup O_{GG_I}$ and take $q \in J/I$. Since $J/I = \langle G\rangle/I$ we have a representation $q = \sum_{g\in G}\sum_i l_i g + \sum_{g_I\in G_I}\sum_i \lambda_i g_I \rho_i$ for a Gröbner basis G_I of I. Now using Buchbergers criterion 1.46 we have that there is $g \in G$ such that $\mathtt{lt}(q) = w\mathtt{lt}(g)$ for some $w \in \langle \mathbf{X}\rangle$, showing that any $q \in J/I$ reduces to zero. By 3.61 G is a Gröbner basis. q.e.d.

3.64 Algorithm.

Input: $E \subseteq \mathbb{K}\langle \mathbf{X}\rangle \setminus \{0\}$, a generating set for J, normal with respect to I, G_I, a Gröbner basis for I

Output: G, a Gröbner basis for J

Start with $G = E$

Set $S = \{\frac{1}{\mathtt{lc}(g)}g - \frac{1}{\mathtt{lc}(g')}wg' \mid g, g' \in G, g \neq g', w \in \langle \mathbf{X}\rangle, \mathtt{lt}(g) \equiv w\mathtt{lt}(g')\} \cup \{\frac{1}{\mathtt{lc}(g)}wg - \frac{1}{\mathtt{lc}(g')}g'r' \mid g \in G, g' \in G_I, w, r' \in \langle \mathbf{X}\rangle, w\mathtt{lt}(g) \equiv \mathtt{lt}(g')r'\}$

while $S \neq \emptyset$ **do**

Take $s \in S$ and set $S = S \setminus \{s\}$

Compute $\overline{s} = lnf(s)$.

if $\overline{s} \neq 0$ **then**

$S = S \cup \{\frac{1}{\mathtt{lc}(g)}g - \frac{1}{\mathtt{lc}(\overline{s})}w\overline{s} \mid g \in G, w \in \langle \mathbf{X}\rangle, \mathtt{lt}(g) \equiv w\mathtt{lt}(\overline{s})\} \cup \{\frac{1}{\mathtt{lc}(\overline{s})}w\overline{s} - \frac{1}{\mathtt{lc}(g')}g'r' \mid g' \in G_I, w, r' \in \langle \mathbf{X}\rangle, w\mathtt{lt}(\overline{s}) \equiv \mathtt{lt}(g')r'\}$

$G = G \cup \{\overline{s}\}$

end if

end while

return G

3.65 Lemma. If J/I has a finite left Gröbner basis Algorithm 3.64 terminates after finitely many steps and returns a reduced Gröbner basis of J/I.

Proof: The correctness follows directly from Proposition 3.63, while termination is ensured by the assumption that there is a finite left Gröbner basis. q.e.d.

3.66 Remark. Since $\mathbb{K}\langle\mathbf{X}\rangle/I$ is not necessarily Noetherian the condition that a finite left Gröbner basis exists is not always satisfied, even if we have a finite generating system. The natural choice to guarantee termination is to apply an degree bound, which will return a truncated Gröbner basis as before.
Moreover, note that Algorithm 3.64 is of Buchberger type, meaning we compute S-polynomials from critical pairs. This allows us to apply the Gebauer-Möller criteria in a similar fashion as before, one has just to take the special forms of obstructions into account.

3.67 Remark. Recall 2.66: Our new method for computing Gröbner bases is a direct counterpart to the non-commutative version of the Buchberger algorithm, that is we search for critical pairs and compute S-polynomials. Since the method to compute left Gröbner bases is also of this type we can use the methods presented in 2.63 to find any of the critical pairs of Remark 3.62, therefore using the letterplace methods to compute left Gröbner bases as well.

We end this section with an application of left Gröbner bases. Assume $I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ is a proper ideal. We want to know if $f \in \mathbb{K}\langle\mathbf{X}\rangle/I$ is left invertible that is there is $g \in \mathbb{K}\langle\mathbf{X}\rangle/I$ such that $gf = 1 \in \mathbb{K}\langle\mathbf{X}\rangle/I$.

3.68 Lemma. Take $f \in \mathbb{K}\langle\mathbf{X}\rangle/I$. Then f is left invertible in $\mathbb{K}\langle\mathbf{X}\rangle/I$ if and only if any Gröbner basis of $\langle f\rangle/I$ contains a non-zero constant.

Proof: Assume $\langle f\rangle/I$ contains a non-zero constant $c \in \mathbb{K}$. Since f is a generator we have $gf = c \in \mathbb{K}\langle\mathbf{X}\rangle/I$ for some $g \in \mathbb{K}\langle\mathbf{X}\rangle/I$ that is f is invertible with inverse $\frac{1}{c}g$. On the other hand if f is invertible we have $1 = gf \in \langle f\rangle/I$ for some $g \in \mathbb{K}\langle\mathbf{X}\rangle/I$. So any Gröbner basis G of $\langle f\rangle/I$ must contain a $g \in G$ such that g is a suffix of 1, that is $g \in \mathbb{K} \setminus \{0\}$.q.e.d.

3.69 Corollary. If $\langle f\rangle/I \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle/I$ has an infinite Gröbner basis then f is not invertible.

Proof: Assume f is invertible that is any Gröbner basis contains a non-zero constant. Therefore $1 \in \langle f\rangle/I$ is a finite Gröbner basis showing that each Gröbner basis is indeed finite. q.e.d.

Assuming $\mathtt{NF}(f, I) \neq 0$ one can use Lemma 3.68 to obtain an inverse of f by keeping track of the computations in Algorithm 3.64, therefore identifying the element in O_{GG_I} that leads to 1. The coefficient w of f in $\frac{1}{\mathtt{lc}(g)}wg - \frac{1}{\mathtt{lc}(g')}g'r'$ will then be a left inverse of f.

3.5 Conclusion

Since it is rather common to work with degree bounds to guarantee termination of the non-commutative Gröbner basis procedure truncated Gröbner basis are

commonly used. In [Stu10] the utility of those truncated bases for computation of the $\mathbb{K}$-dimension and especially for answering the question whether or not the dimension is finite was presented.

Also the notion of elimination orderings and the applications are established in commutative as well as in non-commutative computer algebra. The method to compute syzygies of modules over non-commutative rings and especially the free algebra was introduced in [KB07], as mentioned before. Moreover, the computation of dimension in finitely presented factors of the free algebra was presented in [Stu10] and the methods used go back to [Ufn95], [Ani85] and [GI89].

We like to point out that there was a parallel development for computations of right ideals in factors of the free algebra in [Xiu12], which in theory can also be applied for left ideals (for example by using the opposite algebra).

It is important to note that most computer algebra systems are not able to handle applications of the Gröbner basics. Noteworthy, there is a implementation in ApCoCoA [ApC13] done by Xingqiang Xiu.
It is our intention to use the computer algebra system Singular to implement the methods presented here, thereby creating an efficient subsystem which is able to handle many problems and applications which rely on Gröbner bases. In the next chapter we will give an introduction to the implementation of these methods and demonstrate these methods on interesting examples.

4 Implementation, Applications and Examples

In this chapter we present the implementation and the procedures briefly. Note that there is a section about letterplace in the online manual [DGPS12b] of SINGULAR, which will include our procedures as soon as they are released.
We then present some interesting problems which we tried to solve. We do this not only to present our implementation, but to also stimulate further studies of those cases.

4.1 Overview on the Implementation

SINGULAR is a computer algebra system for polynomial computations, with special emphasis on commutative and non-commutative algebra, algebraic geometry, and singularity theory (see [DGPS12a]).

SINGULAR provides a kernel with highly efficient core algorithms as well as advanced algorithms, contained in currently more than 90 libraries.

To use the structure of SINGULAR the implementation of our methods is divided into two parts:

1. The main algorithm for computations of Gröbner bases of ideals of the free algebra as well as left Gröbner bases of factors of the free algebra are parts of the SINGULAR kernel. This allows the user to use the internal data structure and makes the computations faster and more efficient. The implementation will allow to use the graded lexicographical ordering, weighted degree orderings and the ordering `Elim` introduced in 1.27, as well as any ordering given by a matrix.

2. The algorithms for methods that rely on Gröbner basis computation are implemented in the libraries `freegb.lib` and `fpadim.lib` and the user has to call those in order to use our methods.

In the following we give a small overview over those functions. For a detailed description we refer again to the online manual [DGPS12b] and we like to point out that SINGULAR will always print a small example for the function `functionname` if the user types

`example functionname;`

into the shell.

4.1.1 freegb.lib

The library `freegb.lib` allows the user to create letterplace rings and use most of the algorithms related to the free algebra. A complete introduction is given in [LL09] and in the online-manual [DGPS12b].

Here is a short list of of the newest functions:

- `makeletterplaceRing` [*Elim, WO, MO*](d):
  Depending on the *basering* this function creates a letterplace ring with a degree bound d, which has to be specified. The names of the variables are taken from the basering. If none of the extension is set the degree lexicographical ordering is chosen, while `Elim` sets the elimination ordering $<_{Elim}$, `WP` a weighted degree ordering and `MO` a matrix ordering.
  If the created ring is set as the new basering the user is able to do basic arithmetics over the letterplace ring.

- `lpGroebner`(I):
  Given a letterplace ideal I via generators the function `lpGroebner` computes a Gröbner basis of the ideal up to the degree bound specified by the letterplace ring.

- `lpLeftGB`(J, I):
  Given a set of polynomials J and a Gröbner basis for an ideal I this function computes a left Gröbner basis of the left ideal $\langle J\rangle \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle/I$ up to the degree bound specified by the letterplace ring.

- `lpNF`(p, I):
  This function computes a normal form of a polynomial p with respect to a set of polynomials I. Note that I does not necessarily need to be a Gröbner basis. Then p will be reduced with respect to the set I.

- `lpLeftNF`(p, J, I):
  For a polynomial p and a set of generators J of a left ideal `lpLeftNF` computes a left normal form of p with respect to $\langle J\rangle$.

- `lpSyzygies`(I):
  The function `lpSyzygies` computes the syzygy module for I, a given set of polynomials. Only syzygies which respect the specified degree bound are returned. Again the polynomials of I do not need to form a Gröbner basis.

- `lpIntersection`(I, J):
  For two generating sets of ideals I and J this function returns a Gröbner basis for the intersection of those ideals.

- `lpHomKernel`(I):
  This function computes the kernel of a homomorphism between two finitely presented algebras. Therefore one needs to specify two letterplace rings, both containing a set of polynomials which generate the ideal one likes to factor out. Moreover, a set of polynomials I building the image of the homomorphism is needed.

- `lpConjugatorSearch`(p, q, I):
  Given two elements p and q of a finitely presented group isomorphic to $\mathbb{K}\langle\mathbf{X}\rangle/I$ this algorithm determines whether or not those elements are conjugated and if so it returns a conjugator. If the elements are not conjugated zero will be returned.

4.1.2 fpadim.lib

The `fpadim.lib` contains all procedures regarding dimension computations for finitely presented algebras. A full description of the older routines can be found in [Stu10]. Again we give a short overview on the new procedures.

- `lpGKDim`(I):
  For a given set of generators I this function computes the Gel'fand-Kirillov dimension of $\mathbb{K}\langle\mathbf{X}\rangle/\langle I\rangle$. If the dimension is infinite -1 is returned. For this procedure I is supposed to be a Gröbner basis for $\langle I\rangle$. However, if a truncated Gröbner basis is given as input, the returned value is an upper bound for the Gel'fand-Kirillov dimension.

- `lpGlDBound`:
  This procedure computes an upper bound for the global dimension of $\mathbb{K}\langle\mathbf{X}\rangle/I$. It can be called with a complete or a truncated Gröbner basis, with the bound being more accurate if a full Gröbner basis is known.

4.1.3 Other computer algebra systems

Among the large variety of computer algebra systems we like to mention three of them which are also able to deal with the free algebra.

- Magma:
  The well-known computer algebra system Magma [BCP97] is able to construct free algebras over arbitrary fields, do basic arithemtics, compute Gröbner bases and normal forms. Moreover, the user can define mappings into other associative algebras.

- GAP:
  The library `GBNP` ([Coh07]) of the computer algebra system GAP [GAP13] also allows the user to handle free algebras. Besides the computations of Gröbner bases there are procedures to compute the $\mathbb{K}$-dimension as well as the growth of an algebra $\mathbb{K}\langle \mathbf{X} \rangle / I$.

- ApCoCoA:
  The package `gbmr` for ApCoCoA contains several functions for basic computations and Groebner basis computations in non-commutative algebras, such as finitely generated free monoid rings over the field of rational numbers Q or over finite fields. The development of this package is very recent and a large functionality is provided. We refer to [ApC13] for details.

Of course there are more computer algebra systems and some of them offer functionality for the free algebra. Not all of them are still further developed and alongside Singular the three systems mentioned above offer the reachest functionality for the free algebra.

A special mentioning should be made for Sage [S$^+$13] which is a system that combines many existing open-source packages into a common Python-based interface. For most polynomial computations Sage uses the routines of Singular and in line with our cooperation they intend to use our procedures for computations over the free algebra. Already there is an experimental interface which uses the old letterplace routines for computation of homogeneous Gröbner bases.

4.2 Examples and Applications

The goal of this section is to present problems which are challenging to solve. In fact we could not solve many of the examples and at least from a computational point of view those problems are still open. We like to initiate further studies as it is our belief that our approach is promising and with the development of faster and better computers more problems will become solvable.

In order to make the tests reproducible, we used the new SDEvalv2 framework ([HLN13]), created by Albert Heinle of the SymbolicData project ([BG00]) for our benchmarking. It means that the input polynomials have been put into the system SymbolicData. Then, for each computer algebra system the files to be executed were generated by the SymbolicData using scripts, written by ourselves for this purpose. With the help of SDEvalv2 the *computing task* was formed, put to the compute server, executed and evaluated. The functions of SymbolicData as well as the data are free to use. In such a way our comparison is easily and trustfully reproducible by any other person. Note, that among other the function, which is used to measure the time, can be customized within this approach.

The examples we present here are all available at the SymbolicData database. All tests were performed on a PC equipped with two Intel Core i7 Quadcore Processor (8×2933 MHz) with 16GB RAM running Linux.

4.2.1 Generalized tetrahedron groups

A generalized tetrahedron groups is defined to be a group admitting a presentation $\langle x, y, z \mid x^l = y^m = z^n = W_1^p(x, y) = W_2^q(y, z) = W_3^r(x, z) = 1\rangle$, where $l, m, n, p, q, r \geq 2$ and each $W_i(a, b)$ is a cyclically reduced word involving both a and b. These groups appear in many contexts, not least as fundamental groups of certain hyperbolic orbifolds or as subgroups of generalized triangle groups.

Those groups are well studied, for example the results of [EHRT02], [ERST00], [HMT95] and [RS02] show that up to equivalence there are only generalized tetrahedron groups which have a presentation of the form $\langle x, y, z \mid x^l = y^m = z^n = W_1^2(x, y) = (y^\gamma z^\delta)^2 = (x^\alpha, z^\beta)^2 = 1\rangle$ with $W_1(x, y) = x^{\alpha_1} y^{\beta_1} \cdots x^{\alpha_k} y^{\beta_k}, k \geq 1, l, m, n \geq 2, 1 \leq \alpha_1, \ldots, \alpha_k, \alpha < l, 1 \leq \beta_1, \ldots, \beta_k, \gamma < m$ and $1 \leq \delta, \beta < n$.

Tsaranov classified in [Tsa89] the finite generalized tetrahedron groups with $k = 1$ and showed that there are 5 equivalence classes. Numerical calculations can also be found in [Run98].

In [FHH+08] Rosenberger e.a. presented a classification of all finite generalized tetrahedron groups. The list contains 32 equivalence classes and the order of the largest group is 849346560. The methods used there involve group theory to identify sub- and factor groups. By obtaining their index in the group considered and knowing the order of the identified group one gets the order of the whole group.

We like to apply our methods to reconstruct those examples and verify the results by using our methods.

In table 4.1 we present the relations as well as our results. Note that the relations presented in the table are all equal to one. The timings presented is the time we needed to compute a Gröbner basis only.

The table shows that we managed to solve more than half of the problems. The problems marked with † ran out of memory after some time, while the computation for the two examples marked with $\star$ were canceled after three days of run time. While none of the truncated Gröbner bases had a large number of elements, meaning the number of elements is below 1000, the degree bound we set was never enough to proof finiteness and at some point the computation exceeded the memory of our computer.

Example	Relations	GB	Order	Timing
1	$x^2, y^3, z^2, (xyxy^2)^2, (yz)^2, (xz)^2$	19	48	0.59
2	$x^2, y^3, z^3, (xyxy^2)^2, (yz)^2, (xz)^2$	45	120	0.61
3	$x^2, y^3, z^4, (xyxy^2)^2, (yz)^2, (xz)^2$	110	384	3.65
4	$x^2, y^3, z^5, (xyxy^2)^2, (yz)^2, (xz)^2$	807	14400	0.14
5	$x^2, y^3, z^2, (xyxyxy^2)^2, (yz)^2, (xz)^2$	31	96	0.39
6	$x^2, y^3, z^3, (xyxyxy^2)^2, (yz)^2, (xz)^2$	100	384	3.07
7	$x^2, y^3, z^2, (xyxyxyxy^2)^2, (yz)^2, (xz)^2$	40	240	1.14
8	$x^2, y^3, z^3, (xyxyxyxy^2)^2, (yz)^2, (xz)^2$	†	14400	
9	$x^2, y^3, z^2, (xyxyxy^2xy^2)^2, (yz)^2, (xz)^2$	122	1152	2.89
10	$x^2, y^3, z^3, (xyxyxy^2xy^2)^2, (yz)^2, (xz)^2$	†	23040	
11	$x2, y^3, z^2, (xyxyxy^2xyxy^2)^2, (yz)^2, (xz)^2$	†	1440	
12	$x^2, y^3, z^3, (xyxyxy^2xyxy^2)^2, (yz)^2, (xz)^2$	†	345600	
13	$x^2, y^3, z^2, (xyxyxyxyxy^2xy^2)^2, (yz)^2, (xz)^2$	⋆	5760	
14	$x^2, y^3, z^3, (xyxyxyxyxy^2xy^2)^2, (yz)^2, (xz)^2$	†	2764800	
15	$x2, y^3, z^2, (xyxyxy^2xy^2xyxy^2)^2, (yz)^2, (xz)^2$	492	5760	53.41
16	$x^2, y^3, z^2, (xyxyxyxy^2xyxy^2xy^2)^2, (yz)^2, (xz)^2$	†	11520	
17	$x^2, y^3, z^2, (xyxyxyxy^2xy^2xyxy^2xy^2)^2, (yz)^2, (xz)^2$	†	849346560	
18	$x^2, y^4, z^2, (xyxyxy^3)^2, (yz)^2, (xz)^2$	⋆	384	
19	$x^2, y^4, z^3, (xyxyxy^3)^2, (yz)^2, (xz)^2$	†	9216	
20	$x^2, y^5, z^2, (xyxy^2)^2, (yz)^2, (xz)^2$	59	240	1.38
21	$x^2, y^5, z^3, (xyxy^2)^2, (y^2z)^2, (xz)^2$	59	14400	1.50
22	$x^2, y^5, z^2, (xyxyxy^4)^2, (yz)^2, (xz)^2$	249	2400	81.91
23	$x^2, y^5, z^2, (xyxy^2xy^3)^2, (yz)^2, (xz)^2$	462	2400	868.44
24	$x^2, y^5, z^3, (xyxy^2xy^3)^2, (y^2z)^2, (xz)^2$	†	1728000	
25	$x^2, y^5, z^3, (xyxyxy^4)^2, (yz)^2, (xz)^2$	†	1728000	
26	$x^3, y^3, z^2, (xyx^2y^2)^2, (yz)^2, (xz)^2$	116	576	11.97
27	$x^3, y^3, z^2, (xyxy^2)^2, (yz)^2, (xz)^2$	97	360	3.23
28	$x^3, y^3, z^3, (xyx^2y^2)^2, (yz)^2, (xz)^2$	†	11520	
29	$x^3, y^3, z^3, (xyxy^2)^2, (yz)^2, (xz)^2$	684	7200	2225.95
30	$x^3, y^3, z^2, (xyxyx^2y^2)^2, (yz)^2, (xz)^2$	456	2880	308.55
31	$x^3, y^5, z^2, (xyx^2y^2)^2, (y^2z)^2, (xz)^2$	†	43200	
32	$x^3, y^5, z^2, (x^2yxy^4xy^4)^2, (yz)^2, (xz)^2$	†	1728000	

Table 4.1: All finite Tetrahedron groups

4.3 Moore-Penrose Inverse and Drazin Pseudo-Inverse

In [Dra11] the notion of different *pseudo-inverses* for elements of a semi-group S is discussed. We like to present a method to investigate those inverses. Therefore we introduce the notion first.

4.1 Definition. Let S be any multiplicative semi-group.

- Given any specified involution of S, that is a map $\star : S \to S$ which satisfies $\star(ab) = \star(b) \star (a)$ and $\star(\star(a)) = a$ for any $a, b \in S$, then $y \in S$ is called a *Moore-Penrose inverse* of $a \in S$ if $yay = y$, $aya = a$, $\star(ay) = ay$ and $\star(ya) = ya$. We write $a^\dagger$ for the Moore-Penrose inverse of a.
- We call $y \in S$ a *Drazin pseudo-inverse* of $a \in S$ if $yay = y$, $ay = ya$ and $a^{j+1}y = a^j$ for some $j \in \mathbb{N}$. We write a' for the Drazin pseudo-inverse of a.

The problem communicated to us by Drazin is the following: One is interested in finding pairs of trinomials, that is a pair of polynomials (t_1, t_2) of the form $t_i = a_{i,1}m_{i,1} + a_{i,2}m_{i,2} + a_{i,3}m_{i,3}$ with $a_{i,j} \in \mathbb{K} m_{i,j} \in \langle \mathbf{X} \rangle$, such that $t_1 t_2 = 1$. Thereby the monomials of t_1 and t_2 have to satisfy certain conditions.

For the Moore-Penrose situation we consider the algebra $A = \mathbb{K}\langle x, z, a, y\rangle / I$, where $I = \langle yay - y, aya - a, xzx - x, zxz - z, xz - ya, zx - ay\rangle$. Then we have $y = a^\dagger$, $x = z = \star(a)$. We are looking for $p, q, r, s \in \langle a, y, x, z\rangle$ such that $(1 - p + q)(1 - r + s) = 1$ in A. It is easy to see that the set $\{yay - y, aya - a, xzx - x, zxz - z, xz - ya, zx - ay\}$ does not form a Gröbner basis, however a straightforward computations shows that $G = \{xz - ya, zx - ay, yay - y, yax - x, aya - a, ayz - z, zya - z, xay - x\}$ forms a Gröbner basis for I.

We assume that $\mathtt{lm}(1 - p + q) = q$ and $\mathtt{lm}(1 - r + s) = s$. In order to fulfill the condition $(1 - p + q)(1 - r + s) = 1$ we have that $\mathtt{NF}(qs, G) \neq qs$ which implies certain conditions on q and s:

1. The monomials q and s must involve an overlap o.
2. There is $d \in \{yay, yax, aya, ayz, zya, xay, xz, zx\}$ such that $d|qs$. Since we consider q and s as elements of A, that is q and s are normal with respect to I, this implies that $d|o$.

This allows to consider specific leading monomials only, since one can derive which overlaps may occur. Given an integer $j \in \mathbb{N}$ we can generate a list of all possible q and s of degree j. For example given a natural number $n \in \mathbb{N}$ with $n > 2$, the pairs of trinomials $(y^{n-1}a - y^{n-2} + 1, y^{n-1}a - y^{n-2} - 1)$ and $(ay^{n-1} - y^{n-2} + 1, ay^{n-1} - y^{n-2} - 1)$ will always multiply to one modulo $yay - y$ (this can easily be computed using two reduction steps).

It is easy to see that, in general, more relations lead to more possible overlaps which have to be considered, thus extending the list of possible pairs. However, there are only finitely many choices for a fixed degree d and one can study low degree cases to get a general idea. After a series of intensive computer algebra supported computations, performed by us, a new class of pseudo-inverses was derived by Drazin in the paper [Dra11].

4.4 Quotients of the Modular Group

The modular group is isomorphic to the free product of the cyclic groups C_2 and C_3, which gives its natural and shortest presentation: $\{x, y | x^2, y^3\}$. One-relator quotients of this group, that is one adds another relation $w(x, y)$ to the given presentation, are especially interesting, since many groups have been identified to be such a one-relator quotient, as works of Hamilton [Ham56] and Miller [Mil01] show.

In [CHN11] those groups were studied, based on the work of Conders [Con86] and the authors tried quite succesfully to find the order of those groups. Again using our methods we try to reproduce those results.

The work [CHN11] presents 48 relations which are called the *hard* cases, meaning the question whether or not the group is finite is not easy to answer. Except for 5 the authors can solve these problem by investigating subgroups and quotients.

To study those examples one changes the presentation of the group to $\{u, v | (vu^1v)^2, (u^1v)^3\}$ by using the transformation $u = xy$ and $v = xy^{-1}$. The additional relators are presented in table 4.2.

Since the relations do not reveal a direct inverse of the generator one has to add extra variables for the inverses. This can be done by adding relations to the generating set. Of course this makes the computations even harder.

The studies in [CHN11] leaves the examples 31, 33, 37, 40 and 43 unsolved, but the authors managed to establish lower bounds for the order of those groups with the smallest one being example 33 with an lower bound of 124488.

Our methods were applied to this example. A straightforward approach, as expected, was not succesfull.

A better way to start the computation is to choose a different presentation of the generating system. Since we have inverses of the generators we can multiply to get terms of at least nearly equal total degree. For example the relation $u^4v^2u^2v^4u^2vuv^2 - 1$ translates to $u^4v^2u^2v - V^2UVU^2V^3$, where U denotes the inverse of u and V of v.

Our final effort was to try pattern matching: Assume we have found a truncated Gröbner basis G_t. If a word $w \in \langle \mathbf{X} \rangle$ appears with a certain frequency as a

Example	Additional Relator
1	$(u^3vuv^2)^2$
2	$(u^2vuv)^3$
3	$(u^5vuv)^2$
4	$(u^5v^3)^2$
5	$(u^4vu^2v)^2$
6	$u^3vu^3vu^3v^2uv^2$
7	$u^3vu^3vu^2v^3u^2v$
8	$u^3vu^3v^2uv^3uv^2$
9	$(u^3vu^2v^2)^2$
10	$(u^3v^2uv^2)^2$
11	$(u^2vu^2vuv)^2$
12	$u^{10}uv^2uvuv^2$
13	$u^8v^2uvuvuv^2$
14	$u^8vuvuv^2u^2v^2$
15	$(u^6vuv)^2$
16	$u^6vuv^6u^2v^2$
17	$(u^5vu^2v)^2$
18	$u^5vu^2v^2uv^5uv$
19	$u^5vuvuvuv^5uv$
20	u^5vuvuv^5uvuv
21	$u^5v^2u^2v^5u^2v^2$
22	$u^4vu^3v^3uv^4uv$
23	$u^4vu^2vuvuv^2uv^4$
24	$u^4vu^2vuv^2uv^4uv$

Example	Additional Relator
25	$u^4vu^2vuv^4uv^2uv$
26	$u^4vu^2v^2uv^4uvuv$
27	$u^4vuvu^2v^2uvuv^4$
28	$u^4vuvuvuv^4u^2v^2$
29	$u^4vuvuv^4u^3v^3$
30	$u^4vuv^2u^2vuv^4uv$
31	$u^4vuv^4u^3vuv^3$
32	$u^4vuv^4uvu^4v^2$
33	$u^4v^2u^2v^4u^2vuv^2$
34	$(u^4v^2uv^2)^2$
35	$u^4v^2uv^2u^2vu^2v^4$
36	$u^4v^3uvuvu^3v^4$
37	$u^3vu^2vu^2v^2uv^2uv^3$
38	$u^3vu^2vuv^2uv^3u^2v^2$
39	$u^3vu^2vuv^2uv^3uvuv$
40	$u^3vu^2v^2uv^3u^2vuv^2$
41	$u^3vu^2v^3u^3v^2uv^3$
42	$u^3vuvu^3v^3uvuv^3$
43	$u^3vuvuv^3u^2vuvuv^2$
44	$u^3vuv^3u^2vuvuvuv^2$
45	$u^3vuv^3u^2v^3u^3v^2$
46	$u^3v^2u^2vuvuv^2u^2v^3$
47	$u^3v^2uvu^2v^3u^2vuv^2$
48	$(u^2vuvu^2v^2)^2$

Table 4.2: Additional Relators for one-relator quotients

subword of terms of elements of G_t then we add a new variable y and the relation $w - y$. If the choice of w was good the new variable reduces the total degree needed for the computation. Of course there is no way to know a priori how good the choice will be and the procedure is a *try-and-error* method.

It turned out, that each Gröbner basis computation ran out of memory after some time, even if the dimension is known to be finite (and hence also the Gröbner basis). To investigate these problems we computed truncated Gröbner bases and it turned out that the size of the Gröbner bases just grew very large. While the trick of substitution helped to keep the degree down at the cost of adding a new variable, the size of a truncated Gröbner bases was already bigger at lower degree.

Despite the fact that at the time being no solution could have been found, it should be possible to compute a Gröbner basis at least for the groups known to be finite. With a faster computer the methods mentioned here should allow the computation of those and therefore allowing to compute the order of those groups. In our opinion, the questions, raised in this section, can be answered by combining group-theoretic insights with computer algebra approach.

4.5 Fibonacci Groups

In [BV03] the class of cyclically presented groups which contain Fibonacci groups and Sieradski groups is studied. Those groups can be presented as $G_n(m,k) = \langle x_1, \ldots, x_n \mid x_i x_{i+m} = x_{i+k}, 1 \leq i \leq n \rangle$, where $0 < m < k < n$ and all indices are taken modulo n and take up their values from the set $\{1, \ldots, n\}$.

Using group-theoretic algorithms implemented in GAP the authors studied the question of the order of those groups. We like to verify those computations using our methods.

Since the relations do not allow to determine a inverse for the generators one has to add extra generators for the inverses, as explained before. This leads to the problem that one gets many generators even for small values of n.

In table 4.3 we present the examples and our findings, which confirm the ones in [BV03]. According to [BV03] the group $G_6(1,2)$ has infinite order and our data suggests that the representation most likely holds an infinite Gröbner basis. However, we were not successful in proving this conjecture. Moreover, we tried to find the order of $G_7(1,3)$, which was not found by the authors. With an degree bound of 8 the truncated Gröbner basis for this examples contains 108577 elements and it contains also polynomials of degree 8. Thus one has to increase the degree bound to 15 which is beyond our capacities at the moment.

In 4.3 we present our findings which confirm the results in [BV03]. Note that we have sorted the list such that the isomorphic groups are next to each other.

Example	**Order**	**Size of GB**
$G_5(1,2)$	11	100
$G_5(1,4)$	11	100
$G_5(2,3)$	11	100
$G_5(2,4)$	11	100
$G_5(1,3)$	120	180
$G_5(3,4)$	120	180
$G_6(1,3)$	7	18
$G_6(1,4)$	7	18
$G_6(2,3)$	9	178
$G_6(2,5)$	9	178
$G_6(3,4)$	56	178
$G_6(3,5)$	56	178
$G_7(1,2)$	29	192
$G_7(1,6)$	29	192
$G_7(2,4)$	29	192
$G_7(2,5)$	29	192
$G_7(3,4)$	29	192
$G_7(3,6)$	29	192
$G_8(1,4)$	17	65
$G_8(1,5)$	17	65
$G_8(3,4)$	17	65
$G_8(3,7)$	17	65

Table 4.3: Some Examples of Fibonacci Groups

As 4.3 shows many of the groups have a relatively small order, even in 8 generators. We have to mention that $G_8(1,3)$ has order 295245 which is again beyond our capacities. But it would be worth investigating larger numbers of generators provided there exists a conjecture that one of those groups will be of small order again. However, a first investigation for the groups with $n = 9$ revealed no such phenomenon.

4.6 Comparison to other Systems

We will now present some important examples and compare our timings with those given by the implementation of letterplace Gröbner bases by Viktor Levandovskyy in the current distribution of SINGULAR, as well as with the implementations in GAP and MAGMA. We must mention that the older implementation in SINGULAR as presented in [LL09] has only been released for graded ideals; its functionality with non-graded ideals is experimental.

Note that the implementation of the LETTERPLACE:DVEC algorithm is not yet distributed with SINGULAR. The merge of our development branch with the main branch of SINGULAR will be done soon.

All tests were performed on a PC equipped with two Intel Core i7 Quadcore Processor (8×2933 MHz) with 16GB RAM running Linux. We used MAGMA V2.18-12 [BCP97], GAP Version 4.5.6 [GAP13] with the package GBNP, version 1.0.1 and SINGULAR version 3-1-6.

In [LL09] the authors used external time measuring for the whole computation via `/usr/bin/time` command. This included the initializing of a computer algebra system as well as the loading of standard libraries. Here we use IEEE standard for measuring (POSIX.2) and present the timings from the *system* record of the time output.

In the following tables selected resulting timings are presented. Sing 1 refers to the implementation by Viktor Levandovskyy, currently distributed with SINGULAR, while Sing 2 is the new implementation using distance vectors. Results are presented in seconds. By † we denote the situation when the computation run out of memory after the indicated time.

4.6.1 Examples

Many of the examples are explained in detail in [LL09] or [Stu10] and we use the same notation. In the following we explain only the new ones.

One-relator quotients
All the examples presented in 4.2 are part of the SYMBOLICDATA database. The enumeration is chosen according to the paper and the examples are denoted by

H_i. We have chosen a few ones for comparison and added a degree bound such that all the system were able to solve the problem and return a truncated Gröbner basis.

LS
The examples LS_5d9 and LS_6d10 were presented to us during discussions with Roberto La Scala and are connected to Clifford algebras. Infinite Gröbner bases are expected from this generating sets, therefore degree bounds are employed. The first number denotes the number of generators, while the number following the d denotes the degree bound.

The results show that our implementation is a big improvement to the older letterplace implementation. However, the other systems are similarly efficient. We like to point out that MAGMA is not available as free software and a license has to be acquired.
In the next section we will discuss possibilities for improvements to our methods.

All these examples are easily reproducible using the SYMBOLICDATA database. We have entered over 70 examples and the database will

4.7 Future Work and Conclusion

Our primary goal for the near future is of course the release of our implementation within one of the next updates of SINGULAR and allowing the user to apply our methods to whatever example he or she might consider interesting.

We like to mention that there are many ways to improve our implementation. Of course, our procedures will benefit from any improvement to the SINGULAR kernel and the internal data structure. Besides that we have some ideas which will allow us to optimize memory usage as well as handling of stored polynomials. For example the multiplication of polynomials and the need to save shifted monomials can be optimized further and these updates are currently under development by Benjamin Schnitzler. Our goal regarding orderings is to allow a fast implementation of as many orderings as possible, since the usage of matrices to represent orderings is not as efficient as the implementation of a strategy optimized for a given ordering.

There are some methods we could not investigate in the frame of this work, for example the computation of Gröbner bases for modules or free resolutions of finitely presented modules. But it is possible to adapt our methods to work in the setup of modules and allow new applications to be studied.

Recent studies have investigated the question if the letterplace approach can be applied to other fields of interest. In the very recent bachelor thesis of Bastian Haase ([Haa13]) *multi-letterplace* rings and the application of Gröbner bases theory to these rings are studied. It turned out, that the letterplace ring is the

Example	Sing 1	Sing 2	Magma	GAP
$2tri\_4v7d$	4.10	1.75	1.40	31.67
$3nilp\_d6$	0.41	0.29	0.96	4.76
$3nilp\_d10$	2410.15†	36.65	2.89	31.08
$4nilp\_d8$	380.23†	747.95	10.25	1133.82
$Braid3\_11$	273.40†	15.73	1.52	185.39
$Braid4\_11$	51.82	3.10	1.14	31.97
$plBraid3d\_6$	0.18	0.08	0.91	926.80
$lp1\_10$	31.31	2.33	1.00	11.10
$lv2d10$	0.23	0.15	0.78	3.29
s_e6d10	10.56	1.84	1.12	12.45
s_e6d13	976.32	44.74	7.81	274.63
$s\_eha112d10$	1.12	0.26	0.96	6.20
$s\_eha112d12$	462.36	4.19	1.40	62.40
s_f4_d10	4.35	0.58	0.97	5.35
s_f4_d15	1103.33 †	147.31	13.54	2241.62
s_ha11_d10	2.18	0.32	0.81	3.51
LS_5d9	23.46	2.49	0.79	2.90
LS_6d10	411.33 †	704.97	16.86	372.06
$C\_4\_1\_7a$	576.44	59.47	7.61	2491.09
$C\_4\_1\_7W$	3.23	1.19	0.91	5.76
$C\_4\_1\_7X$	7.44	2.20	6.64	51.95
$C\_4\_1\_7Y$	0.09	0.09	0.91	2.91
$C\_4\_1\_7Z$	66.92	11.86	4.82	173.44
H_5	0.62	0.24	0.62	2.90
H_8	0.67	0.28	3.07	2.94
H_19	0.88	0.32	0.62	2.99
H_26	0.91	0.33	2.30	2.96
H_33	0.92	0.35	2.27	3.00
H_37	0.86	0.32	0.68	2.89
H_40	0.98	0.29	0.62	2.89
H_48	0.88	0.31	0.62	2.91

natural ring for studying systems of nonlinear difference equations with constant coefficients for instance, with the help of Gröbner bases. Moreover, the rich structure of the letterplace ring which can be exploited for many applications. We like to point out that our methods here use only a small part of the huge letterplace ring. We believe, that further studies will lead to new applications of the letterplace approach in different fields of science.

Bibliography

[AAG99] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public key cryptography. *Math. Res. Lett.*, 6:287–291, 1999.

[AL88] Joachim Apel and Wolfgang Lassner. An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *J. Symbolic Compututation*, 6(2-3):361–370, 1988. Computational aspects of commutative algebra.

[Ani85] David J. Anick. On monomial algebras of finite global dimension. *Transactions of The American Mathematical Society*, 291, 1985. `http://dx.doi.org/10.2307/1999910`.

[Ani86] David J. Anick. On the homology of associative algebras. *Transactions of The American Mathematical Society*, 296:641–641, 1986. `http://dx.doi.org/10.2307/2000383`.

[ApC13] ApCoCoATeam. Applied Computations in Commutative Algebra, 2013. `www.apcocoa.org`.

[Ape00] Joachim Apel. Computational ideal theory in finitely generated extension rings. *Theoret. Comput. Sci.*, 244(1-2):1–33, 2000.

[B+06] Jörgen Backelin et al. The Gröbner basis calculator Bergman, 2006.

[BB98] Miguel Angel Borges and Mijail Borges. Gröbner bases property on elimination ideal in the non-commutative case. In B. Buchberger and F. Winkler, editors, *Gröbner bases and applications*, pages 323–337. Cambridge University Press, 1998.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Computation*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Ber78] George Bergman. The Diamond Lemma for ring theory. *Adv. Math.*, 29:178–218, 1978.

[BG00] Olaf Bachmann and Hans-Gert Gräbe. The SYMBOLICDATA project. In *Reports on Computer Algebra*, volume 27. Centre for Computer Algebra, University of Kaiserslautern, 2000. http://www.mathematik.uni-kl.de/~zca.

[BV03] Valerij Bardakov and Andrei Vesnin. A generalization of Fibonacci groups. *Algebra and Logic*, 42(2):73–91, 2003. http://dx.doi.org/10.1023/A%3A1023346206070.

[CHN11] Marston Conder, George Havas, and Michael Frederick Newman. On one-relator quotients of the modular group., 2011. Cambridge University Press. London Mathematical Society Lecture Note Series 387, 183-197.

[Coh07] Arjeh M. Cohen. Non-commutative polynomial computations. http://www.win.tue.nl/~amc/pub/grobner/gbnp.pdf, 2007. TU Eindhoven. Technical Report.

[Con86] Marston Conder. *Three-relator Quotients of the Modular Group.* Report series. University of Auckland, Department of Mathematics and Statistics, 1986.

[CPU99] Svetlana Cojocaru, Alexander Podoplelov, and Viktor Ufnarovskij. Non-commutative Gröbner bases and Anick's resolution. In P. Dräxler, editor, *Computational methods for representations of groups and algebras. Proc. of the Euroconference in Essen, Germany, April 1997*, pages 29–60. Birkhäuser, 1999.

[CSRL01] Thomas H. Cormen, Clifford Stein, Ronald L. Rivest, and Charles E. Leiserson. *Introduction to Algorithms.* McGraw-Hill Higher Education, 2nd edition, 2001.

[DGPS12a] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR 3-1-6 — A computer algebra system for polynomial computations. 2012. http://www.singular.uni-kl.de.

[DGPS12b] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR online manual. 2012. http://www.singular.uni-kl.de/index.php/singular-manual.html.

[Dra11] Michael P. Drazin. A class of outer generalized inverses. *Linear Algebra and its Applications*, 436, 2011. http://www.sciencedirect.com/science/article/pii/S0024379511006367.

[EHRT02] Martin Edjvet, James Howie, Gerhard Rosenberger, and Richard M. Thomas. Finite generalized tetrahedron groups with a high-power relator. *Geometriae Dedicata*, 94:111139, 2002.

[ERST00] Martin Edjvet, Gerhard Rosenberger, Michael Stille, and Richard M. Thomas. On certain finite generalized tetrahedron groups. *Computational and Geometric Aspects of Modern Algebra*, 275:5465, 2000. http://dx.doi.org/10.1017/CBO9780511600609.005.

[EW07] Gareth A. Evans and Christopher D. Wensley. Complete involutive rewriting systems. *J. Symbolic Computation*, 42(11-12):1034–1051, 2007. http://dx.doi.org/10.1016/j.jsc.2007.07.005.

[FHH+08] Benjamin Fine, Miriam Hahn, Alexander Hulpke, Volker große Rebel, Gerhard Rosenberger, and Martin Scheer. All finite generalized tetrahedron groups. *Mathematical Preprints*, 2008. http://hdl.handle.net/2003/25188.

[GAP13] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.6.4*, 2013. http://www.gap-system.org.

[Gar07] David Garber. Braid group cryptography. *CoRR*, abs/0711.3941, 2007. http://arxiv.org/abs/0711.3941.

[GGK+06] Lothar Gerritzen, Dorian Goldfeld, Martin Kreuzer, Gerhard Rosenberger, and Vladimir Shpilrain. *Algebraic methods in cryptography*. Contemp. Math. 418. Amer. Math. Soc., Providence, RI, 2006.

[GI89] Tatiana Gateva-Ivanova. Global dimension of associative algebras. In Teo Mora, editor, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 357 of *Lecture Notes in Computer Science*, pages 213–229. Springer Berlin Heidelberg, 1989. http://dx.doi.org/10.1007/3-540-51083-4_61.

[GM88] Rüdiger Gebauer and H. Michael Möller. On an installation of Buchberger's algorithm. *J. Symbolic Computation*, 6(2-3):275–286, December 1988. http://dx.doi.org/10.1016/S0747-7171(88)80048-8.

[GP08] Gert-Martin Greuel and Gerhard Pfister. *A* Singular *introduction to commutative algebra*. Springer-Verlag, Berlin, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[Gre93] Edward L. Green. An introduction to non-commutative Gröbner bases. In K. Fischer, editor, *Computational algebra. Papers from the Mid-Atlantic Algebra Conference*, pages 167–190. Dekker. Lect. Notes Pure Appl. Math. 151, 1993.

[Gre96] Edward L. Green. Non-commutative Gröbner bases: A computational and theoretical tool, 1996. Lecture Notes, Holiday Mathematics Symposium, New Mexico State University.

[Gre00] Edward L. Green. Multiplicative Bases, Gröbner Bases, and Right Gröbner Bases. *J. Symbolic Computation*, 29(4/5), 2000.

[Gre03] David J. Green. *Gröbner bases and the computation of group cohomology*. Lecture Notes in Mathematics 1828. Springer, 2003.

[Haa13] Bastian Haase. Multi-letterplace ring, multi-gradings and applications. `http://mira.math.rwth-aachen.de/~Viktor.Levandovskyy/filez/BachelorThesisHaase.pdf`, 2013. Bachelor thesis, RWTH Aachen University.

[Ham56] William Rowan Hamilton. Memorandum respecting a new system of roots of unity. *Phil. Mag. (Ser. 4)*, 12:446, 1856.

[HLN13] Albert Heinle, Viktor Levandovskyy, and Andreas Nareike. Symbolicdata:sdeval - benchmarking for everyone. 2013. submitted.

[HMT95] James Howie, Vassilis Metaftsis, and Richard M. Thomas. Finite generalized triangle groups. *Trans. AMS*, 347:36133623, 1995.

[KB07] Martin Kreuzer and Holger Bluhm. Computation of two-sided syzygies over non-commutative rings. *Contemporary Mathematics*, 421:45–64, 2007. `http://staff.fim.uni-passau.de/~kreuzer/papers/ncsyz.pdf`.

[KLC+00] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju sung Kang, and Choonsik Park. New public key cryptosystems using braid groups. In J. Bellare, editor, *Advances in cryptology – CRYPTO 2000*, pages 166–183, Berlin, 2000. Springer. LNCS 1880.

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.

[KR05] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra. 2.* Springer-Verlag, Berlin, 2005.

[Kro03] Chris Krook. Dimensionality of quotient algebras, 2003. Technical Report.

[KRW90] Abdelilah Kandri-Rody and Volker Weispfenning. Non-commutative Gröbner bases in algebras of solvable type. *J. Symbolic Computation*, 9(1):1 – 26, 1990. `http://www.sciencedirect.com/science/article/pii/S074771710880003X`.

[KX13] Martin Kreuzer and Xingqiang Xiu. Non-Commutative Gebauer-Moeller Criteria. *ArXiv e-prints*, 2013. `http://adsabs.harvard.edu/abs/2013arXiv1302.3805K`.

[Lev05] Viktor Levandovskyy. *Non-commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementation.* PhD thesis, Technische Universität Kaiserslautern, 2005. https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/1670.

[Li12] Huishi Li. *Gröbner Bases in Ring Theory.* World Scientific Publishing Co. Pte. Ltd., 2012.

[LL09] Roberto La Scala and Viktor Levandovskyy. Letterplace ideals and non-commutative Gröbner bases. *J. Symbolic Computation*, 44(10):1374–1393, 2009. http://www.sciencedirect.com/science/article/pii/S0747717109000637.

[Mil01] George Abram Miller. On the groups generated by two operators. *Bulletin of the American Mathematical Society*, 7:424–426, 1901. http://projecteuclid.org/DPubS?service=UI&version=1.0&verb=Display&handle=euclid.bams/1183416688.

[MK02] Viktor D. Mazurov and Evgenii I. Khukhro. *Open problems in group theory: the Kourovka notebook.* Institute of Mathematics, Novosibirsk University, Novosibirsk, 2002.

[Mor86] Teo Mora. Gröbner bases for non-commutative polynomial rings. *Proc. AAECC 3 Lect. N. Comp. Sci*, 229:353–362, 1986.

[Mor88] Teo Mora. Gröbner bases in non-commutative algebras. In *Proceedings of ISSAC conference*, volume 358 of *Lecture Notes in Computer Science*, pages 150–161. Springer, 1988.

[Mor94] Teo Mora. An introduction to commutative and non-commutative Gröbner bases. *Theor. Comp. Sci.*, 134:131–173, 1994.

[MR87] John C. McConnell and J. Chris Robson. *Non-commutative Noetherian Rings.* Pure and Applied Mathematics. John Wiley & Sons, 1987.

[Nor98] Patrik Nordbeck. On some basic applications of Gröbner bases in non-commutative polynomial rings. In *Gröbner Bases and Applications*, pages 463–472. University Press, 1998.

[Rob85] Lorenzo Robbiano. Term orderings on the polynomial ring. In *Lecture Notes in Comput. Sci., 204*, pages 513–517. Springer, 1985.

[RS02] Gerhard Rosenberger and Martin Scheer. Classification of the finite generalized tetrahedron groups. *Contemporary Math.*, 296:207229, 2002.

[Run98] C. Runge. Endliche Tetraedergruppen Der Tsaranov Fall. Diploma thesis, TU Dortmund University, 1998.

[S+13] William A. Stein et al. *Sage Mathematics Software (Version 5.10)*. The Sage Development Team, 2013. http://www.sagemath.org.

[Sca12] Roberto La Scala. Extended letterplace correspondence for non-graded non-commutative ideals and related algorithms. 2012. http://arXiv.org/abs/1206.6027.

[Sim94] Charles C. Sims. *Computation with finitely presented groups*. Encyclopedia of mathematics and its applications. Cambridge University Press, 1994. http://opac.inria.fr/record=b1082972.

[SL13] Roberto La Scala and Viktor Levandovskyy. Skew polynomial rings, Gröbner bases and the letterplace embedding of the free associative algebra. *J. Symbolic Computation*, 48(0):110 – 131, 2013. http://dl.acm.org/citation.cfm?id=2381639.

[Stu10] Grischa Studzinski. Algorithmic computations for factor algebras. Diploma thesis, RWTH Aachen, 2010. http://www.math.rwth-aachen.de/~Grischa.Studzinski/DA.pdf.

[Tra07] Quoc-Nam Tran. A new class of term orders for elimination. *J. Symbolic Computation*, 42(5):533 – 548, 2007. http://www.sciencedirect.com/science/article/pii/S0747717107000314.

[Tsa89] Sergei V. Tsaranov. Finite generalized Coxeter groups. *Algebras, Groups and Geometries*, 6(4):421–452, 1989.

[Ufn89] Victor Ufnarovskij. On the use of graphs for calculating the basis, growth and Hilbert series of associative algebras. (Russian). *Mat. Sb.*, 180:1548–1560, 1989. translation in Math. USSR-Sb., 68:417–428, 1991.

[Ufn95] Victor Ufnarovskij. *Combinatorial and asymptotic methods in algebra*. Itogi Nauki i Tekhniki. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1995.

[Ufn98] Victor Ufnarovskij. Introduction to non-commutative Gröbner bases theory. In B. Buchberger and F. Winkler, editors, *Gröbner bases and applications*, pages 259–280. Cambridge University Press, 1998.

[Ufn08] Victor Ufnarovskij. On the cancellation rule in the homogenization. *Computer Science Journal of Moldova*, 16(1(46)):133–145, 2008.

[Xiu12] Xingqiang Xiu. *Non-Commutative Gröbner Bases and Applications*. PhD thesis, University of Passau, 2012. http://www.opus-bayern.de/uni-passau/volltexte/2012/2682/.