Computation of noncommutative Gröbner bases

Berthold Lorke

Born December 30th, 1994 in Munich, Germany

July 26, 2021

Master's Thesis Mathematics

Advisor: Prof. Dr. Catharina Stroppel

Second Advisor: Dr. Jens Eberhardt

Mathematisches Institut

Mathematisch-Naturwissenschaftliche Fakultät der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Abstract

In this thesis, we discuss noncommutative Gröbner bases and their algorithmic computation, providing concrete examples with the computer algebra system Singular.

It is not only possible to define Gröbner bases for the noncommutative polynomial ring $k\langle X\rangle$, but also more generally for k-algebras A with a multiplicative basis $\mathcal{B}$ and an admissible order $\preceq$, which we will study extensively. This then also includes the case of path algebras kQ for a quiver Q. An important intuition for the meaning of Gröbner bases is related to being able to perform a division with remainder. We will see that such a division is possible to be computed algorithmically. What we also wish is to algorithmically compute a Gröbner basis G for an ideal $I \subseteq A$ given by a finite list of generators. For this, we try to generalize the concepts that are known for $k\langle x_1, \ldots, x_n\rangle$, namely obstructions and S-polynomials, after which we arrive at the algorithm to compute Gröbner bases: Buchberger's procedure. Finally, we will also briefly discuss these concepts in G-algebras, which is a generalization of universal enveloping algebras $\mathrm{U}(\mathfrak{g})$ for a Lie algebra $\mathfrak{g}$, where the setting is similar to the one for commutative Gröbner bases.

Acknowledgements

I am grateful to my advisor, Prof. Dr. Catharina Stroppel, who suggested the topic of this thesis, for her continuous support, and for providing valuable advice. I also want to thank Dr. Jens Eberhardt for agreeing to be the second referee. Especially considering the difficulties during the Corona crisis, I am thankful to my friends from university, with whom I was able to socialize via our math Discord server, where we shared many LaTeX and style tips for our work. Finally, I would like to thank Manuel Hoff for his support and for proofreading.

Contents

Introduction **7**

1. General Gröbner basis theory **11**
1.1. Algebras with multiplicative basis 11
1.2. Admissible orders 16
1.3. Noncommutative polynomials in SINGULAR 25
1.4. Gröbner bases 27

2. Algorithms For Gröbner Bases **33**
2.1. Division with remainder 33
2.2. An example for different reduction strategies 37
2.3. Gröbner representations 40
2.4. Obstructions and S-polynomials 42
2.5. Buchberger's criterion 45
2.6. Buchberger's procedure and interreduction 50
2.7. Further considerations for the general case 59

3. G-Algebras **63**
3.1. Gröbner bases and the non-degeneracy conditions 63
3.2. Checking the non-degeneracy conditions in SINGULAR 64
3.3. Gröbner bases in G-algebras 69

A. Appendix **73**
A.1. Multiplicative bases and semigroups with zero element 73
A.2. Path algebras 75

Introduction

The main concept which this thesis revolves around is the notion of a **Gröbner basis**. Let us try to get an intuition behind what this is by looking at known settings that we can later reframe into the theory of Gröbner bases.

In Euclidean domains, we have by definition the concept of a **division with remainder**. Spelling it out, for the underlying commutative ring A, there exists a valuation function $\ell\colon A \setminus \{0\} \to \mathbb{N}_0$ such that for all $p, q \in A$ we have $\ell(q) \leq \ell(pq)$, and there exist $w, r \in A$ such that $p = wq + r$ such that either $r = 0$ or $\ell(r) < \ell(q)$. This property leads to the fact that A then also is a principal ideal domain, meaning that any ideal I can be generated by a single element, the **greatest common divisor**. In general, this is not unique, but unique up to unit, and often there is some kind of a canonical choice, which is then denoted by $\gcd(I)$. We will see that what lies behind the fact that there always exists a single element that generates a given ideal, is that $\mathbb{N}_0$ is **well-ordered**.

For a more intuitive approach to what a well order is, consider having two elements $a, b \in A$ for which we want to find the generator of the ideal generated by a and b. This can be done algorithmically with the **Euclidean algorithm**: Assume that $\ell(a) \geq \ell(b)$.

1. Choose a representation $a = wb + r$ with $r = 0$ or $\ell(r) < \ell(b)$.
2. If $r \neq 0$, we set $a \leftarrow b$ and $b \leftarrow r$ and return to step 1.
3. If otherwise $r = 0$, we terminate the algorithm and return b.

The reason that this algorithm must terminate, is that every time we have $r \neq 0$ in the algorithm, $\ell(r)$ keeps decreasing strictly, and due to the fact that $\mathbb{N}_0$ is well-ordered, this cannot happen infinitely many times, meaning that r must eventually be 0. To compute the greatest common divisor of an ideal given by a finite set of generators of any size, we can successively compute the greatest common divisor for a pair of elements, reducing the size of the set in each step, until only one element is left.

Let us see this in action with the integers $\mathbb{Z}$. Here, $\ell\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0$ is the map $n \mapsto |n|$. Let $a = 261$ and $b = 48$. We then perform the Euclidean algorithm.

- $261 = 5 \cdot 48 + 21$
- $48 = 2 \cdot 21 + 6$
- $21 = 3 \cdot 6 + 3$
- $6 = 2 \cdot 3 + 0$

We conclude that 3 generates the ideal generated by 261 and 48. As noted before, the greatest common divisor is unique up to unit, so in the case of the integers $\mathbb{Z}$, we have $\mathbb{Z}^\times = \{1, -1\}$, so 3 and -3 are possible greatest common divisors. By convention, "the" greatest common divisor is the positive one, so $\gcd(261, 48) = 3$ in this case.

In this example in the integers $\mathbb{Z}$, it is quite easy to compute the division with remainder in each step of the Euclidean algorithm. In other settings, the computation of the division with remainder might be a little more involved, as is the case for the polynomial ring in one variable $A = k[x]$, which we shall discuss now.

The valuation function in $k[X]$ is just degree. As an example, we shall divide $p = 10x^5 + 24x^4 - 33x^3 - 38x^2 - 6x + 44$ by $q = 5x^3 + 2x^2 - 3x - 6$ by polynomial long division.

$$
\begin{array}{rl}
(10x^5 + 24x^4 - 33x^3 - 38x^2 - 6x + 44) \,/\, (5x^3 + 2x^2 - 3x - 6) = 2x^2 + 4x + (-7) & \\
-(10x^5 + 4x^4 - 6x^3 - 12x^2) & \text{rem. } -3x + 2 \\
\hline
20x^4 - 27x^3 - 26x^2 - 6x + 44 & \\
-(20x^4 + 8x^3 - 12x^2 - 24x) & \\
\hline
-35x^3 - 14x^2 + 18x + 44 & \\
-(35x^3 - 14x^2 + 21x + 42) & \\
\hline
-3x + 2 &
\end{array}
$$

The way this algorithm loosely works, is that we keep looking at divisibility for the leading terms, the biggest occurring monomials, in each successive step. More precisely:

1. We start by seeing if we can write the leading expression $\mathrm{LM}(p)$ of p, as a multiple of the leading expression $\mathrm{LM}(q)$ of q, meaning $\mathrm{LM}(p) = w \cdot \mathrm{LM}(q)$ for w some scalar multiple of a monomial.

2. If this is possible, we subtract $w \cdot q$ from p, and go back to step one. In our case, the first time we reach this step we have $\mathrm{LM}(p) = 10x^3 = 2x^2 \cdot 5x^3 = w \cdot \mathrm{LM}(q)$.

3. Otherwise, we terminate the algorithm, and return what is left after having subtracted multiple times, which is the remainder r.

We get the representation $p = wq + r = (\sum_{i=1}^{e} w_i)q + r$, where the w_i are scalar multiples of monomials. In our case, we have $e = 3$, $w_1 = 2x^2$, $w_2 = 4x$, $w_3 = -7$ and $r := p_3 = -3x + 2$.

We have a method to calculate the division with remainder, and we can therefore also compute a greatest common divisor of a finite set of polynomials, with the same procedure as for the integers $\mathbb{Z}$, the Euclidean algorithm. As noted before, the greatest common divisor is unique up to unit, and in $k[X]$, there exists a unique **monic** one, called "the" greatest common divisor. What we then also notice, is that for any ideal I, we have a vector space complement $k[x] = I \oplus \mathrm{span}_k\{x^i \mid i < \deg(\gcd(I))\}$. This is again due to the fact that we can uniquely decompose any element $f \in k[x]$ as $f = w \cdot \gcd(I) + r$ with $r = 0$ or $\deg(r) < \deg(\gcd(I))$.

Let us summarize. For Euclidean domains, we have the following properties.

- A division with remainder: $p = wq + r$
- A representative of an ideal I, the greatest common divisor: $I = (\gcd(I))$. This can be algorithmically computed with the Euclidean algorithm if the ideal is given by finitely many generators $I = (f_1, \dots, f_r)$.

The k-algebra $k[x]$ has even more structure, and we get even more useful properties.

- The division with remainder has the form $p = wq + r = (\sum_i w_i)q + r$, where the w_i are monomials.
- The division with remainder can be algorithmically computed.
- We have a vector space complement $k[x] = I + \operatorname{span}_k\{x^i \mid i < \deg(\gcd(I))\}$ for any ideal I.

Our goal is separate these properties from the setting of Euclidean domains, and try to generalize the results and procedures for (noncommutative) associative unital k-algebras.

If we try to naively generalize the division algorithm to multivariate polynomial rings, there is no canonical "biggest" monomial, there could be multiple different monomials of same degree. This is where we find the need to introduce some kind of an order $\preceq$ on these monomials. Just as the natural numbers are well-ordered when we think about the valuation function for Euclidean domains, we also find it necessary to well-order the set of monomials. As the valuation is compatible with the multiplication in Euclidean domains, meaning $\ell(q) \leq \ell(pq)$, we also similarly want to have $a \preceq ab$ for monomials a and b, where $\preceq$ is a well order.

What we will try to do is not only look at noncommutative polynomial rings, but also see where we can find the same results for path algebras and the more general setting, k-algebras with a **multiplicative basis** $\mathcal{B}$ and an **admissible order** $\preceq$. The most important concepts that we will come across are (reduced) **Gröbner bases**, generalizing the greatest common divisor, and **Buchberger's procedure**, generalizing the Euclidean algorithm. With the help of the computer algebra system SINGULAR, we can compute Gröbner bases for noncommutative polynomial rings.

$k[x]$	k-algebra with admissibly ordered multiplicative basis $\mathcal{B}$
monomial	element of $\mathcal{B}$
degree	leading term
polynomial long division with remainder	division with remainder by multiple elements
greatest common divisor	(reduced) Gröbner basis
Euclidean algorithm	Buchberger's procedure

Notation

- For the natural numbers, $\mathbb{N}_0$ shall denote the nonnegative integers, and $\mathbb{N}_{>0} = \mathbb{N}_0 \setminus \{0\}$ shall denote the positive integers.
- $[n] := \{1, \dots, n\}$ for $n \in \mathbb{N}_0$, in particular $[0] = \emptyset$.
- $B^A := \{f \colon A \to B\}$ denotes the set of all maps from the set A to the set B.
- k is a field of characteristic 0, with multiplicative units $k^\times = k \setminus \{0\}$.
- A "scalar" will refer to an element in k.
- If not specified otherwise, "k-algebra" means an associative unital k-algebra.
- If not stated otherwise, (X) is the two-sided ideal generated by a subset X of a given k-algebra.
- If I is an ideal of a k-algebra A, we denote by $\overline{a}$ the residue class of a in A/I, and if $M \subseteq A$ is a set, we write $\overline{M} = \{\overline{a} \in A/I \mid a \in M\}$ for the set of all residue classes of elements in M.

1. General Gröbner basis theory

In this chapter, we will cover the basic abstract theory of Gröbner bases. Some aspects of the motivation and intuition behind Gröbner bases might only be apparent after we discuss the algorithmic computation of such, as that is where we take a closer look at performing a division with remainder. This will be discussed in the next chapter.

If not stated otherwise, A is an associative unital k-algebra with unit 1.

1.1. Algebras with multiplicative basis

Definition 1.1 (multiplicative basis)**.** A k-basis $\mathcal{B} \subseteq A$ is called a **multiplicative basis** if $\mathcal{B}_0 := \mathcal{B} \cup \{0\}$, with the multiplicative structure of A, is a semigroup. In other words, we have

$$b \cdot b' \in \mathcal{B} \text{ or } b \cdot b' = 0$$

for all $b, b' \in \mathcal{B}$. The elements in $\mathcal{B}$ are also called **monomials** (even if A is not a polynomial ring). ◁

Definition 1.2 (compatible ideals, monomial ideals)**.** Let A have multiplicative basis $\mathcal{B}$. A two-sided ideal $I \subseteq A$ is called **compatible** with $\mathcal{B}$ if it is generated by elements of the form $b - b'$ for $b, b' \in \mathcal{B}_0$. If the ideal is generated by elements $b \in \mathcal{B}$, that is $b' = 0$ for every such generator, it is called a **monomial ideal**. ◁

Definition 1.3 (algebras generated by monoids)**.** Let $\mathcal{B}$ be a monoid. We define the associative k-algebra $k\mathcal{B}$ as having the underlying k-vector space $\bigoplus_{b \in \mathcal{B}} k \cdot b$ with basis $\mathcal{B}$, and having the multiplicative structure of the k-linear extension of the monoid structure on $\mathcal{B}$. ◁

The k-algebra $k\mathcal{B}$ is indeed unital with unit $1_A = 1_{\mathcal{B}}$, and it has multiplicative basis $\mathcal{B}$, where we have the special situation that we never have $b \cdot b' = 0$ for $b, b' \in \mathcal{B}$.

Proposition 1.4. *If I is a compatible ideal, then A/I has multiplicative basis $\overline{\mathcal{B}} \setminus \{0\}$. If I is a monomial ideal, then A/I has multiplicative basis $\overline{\mathcal{B} \setminus I}$, and we furthermore have a one to one correspondence between $\mathcal{B} \setminus I$ and $\overline{\mathcal{B} \setminus I}$.* ◁

Proof (sketch). Firstly, $\overline{\mathcal{B}} \setminus \{0\}$ generates A/I as $\mathcal{B}$ generates A. What is still to show is that $\overline{\mathcal{B}} \setminus \{0\}$ is linearly independent in A/I. The intuition behind why this is true is that modding out elements of the form $b - b'$ just means that we identify b and b' with each other, and by extension we identify any term that contains b somewhere with the same term with b replaced by b' in the term at that same position. Therefore basis elements only get identified with other basis elements or zero, and for this reason linear

independence gets inherited from $\mathcal{B}$ to $\overline{\mathcal{B}} \setminus \{0\}$. To formalize this argument, we can frame these statements in a more categorical context, which is presented in the appendix in Proposition A.4.

If I is a monomial ideal, the one to one correspondence then between $\mathcal{B} \setminus I$ and $\overline{\mathcal{B} \setminus I}$ follows from pure linear algebra: We are taking the quotient with respect to a linear subspace I spanned by basis elements. □

Example 1.5.

1. If X is a (finite) set, let $\mathcal{B} := \langle X \rangle$ be the free monoid over X, which is the set of all words over X with concatenation as the monoid structure, and the unit is the empty word. This means that $\langle X \rangle = \bigcup_{n \in \mathbb{N}_0} X^{[n]}$, where $X^{[n]}$ are the words of **length** or **degree** n. Note that $X^{[0]} = \{1\}$ contains only the empty word and $X^{[1]} = X$.

   Then $k\mathcal{B} = k\langle X \rangle$ is the non-commutative polynomial ring over k in the variables X with multiplicative basis $\langle X \rangle$.

2. For X a (finite) set, let $\mathcal{B} := [X]$ be the free commutative monoid over X, which consists of the set of all maps $X \to \mathbb{N}_0$ with finite support, with pointwise addition as the monoid structure and the zero map being the unit. For $a \in [X]$, we call $\ell(a) := |a| = \sum_{x \in X} a(x)$ the **degree** of a. It is common to write an element $a \in [X]$ as $\prod_{x \in X} x^{k_x}$ for uniquely determined exponents $k_x \in \mathbb{N}_0$, namely $k_x = a(x)$.

   We then get that $k\mathcal{B} = k[X]$ is the commutative polynomial ring over k in the variables X with multiplicative basis $[X]$.

   In light of Proposition 1.4, we can also view the commutative polynomial ring as the quotient of the non-commutative polynomial ring with a compatible ideal:

   $$k[X] = k\langle X \rangle / (xy - yx \mid x, y \in X) \, .$$

3. Consider the k-algebra $k\langle X \rangle$ with multiplicative basis $\langle X \rangle$ and the monomial ideal $I = (M)$ generated by $M = \{m \in \langle X \rangle \mid \ell(m) = d + 1\}$, the monomials of degree $d + 1$. Then $k\langle X \rangle / I = \overline{k\langle X \rangle_{\leq d}}$ is the ring of polynomials of degree at most d with multiplicative basis $\overline{\{x \in \langle X \rangle \mid \ell(x) \leq d\}}$.

◁

Proposition 1.6. *In a multiplicative basis $\mathcal{B}$ of a unital associative k-algebra, for each $b \in \mathcal{B}$ there exist $l_b \in \mathcal{B}$ and $r_b \in \mathcal{B}$ such that $l_b b = b = b r_b$.* ◁

Proof. We will only do the proof for l_b, as r_b is completely analogous. As $\mathcal{B}$ is a basis, we have $1 = \sum_{j \in J} \lambda_j b_j$ for some finite set J and some $\lambda_j \in k$ and $b_j \in \mathcal{B}$. We now have $b = 1 \cdot b = \sum_{j \in J} \lambda_j b_j b$. As $b_j b \in \mathcal{B}$ for all $j \in J$ this then gives us

$$0 = b - \sum_{j \in J} \lambda_j b_j b = (1 - \sum_{b_j b = b} \lambda_j) b + \sum_{c \in \mathcal{B} \setminus \{b\}} (\sum_{b_j b = c} \lambda_j) c \, .$$

As $\mathcal{B}$ is a basis, we must have that $\sum_{b_j b = c} \lambda_j = 0$ for all $c \in \mathcal{B} \setminus \{b\}$ and that $\sum_{b_j b = b} \lambda_j = 1$. In particular, the sum is not empty, so there indeed exists a $j' \in J$ such that $b_{j'} b = b$, and we can choose $l_b = b_{j'}$. □

Example 1.7.

- If $1 \in \mathcal{B}$, then we have $1b = b1 = b$ for all $b \in \mathcal{B}$. This is therefore true for all k-algebras of the form $k\mathcal{B}$ for a monoid $\mathcal{B}$, in particular for the k-algebra $k\langle X\rangle$ with multiplicative basis $\mathcal{B} = \langle X\rangle$.
- Let A have multiplicative basis $\mathcal{B}$ and consider the k-algebra A^r for some $r \in \mathbb{N}_{>0}$ with pointwise multiplication as the multiplicative structure (A^r is also an A-algebra). We then have multiplicative basis $\mathcal{B}' = \bigcup_{i\in[r]} \mathcal{B} \cdot e_i$, where $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ with 1 at the i-th position. If then $m' \in \mathcal{B}'$, we must have $m' = m \cdot e_i$ for some $m \in \mathcal{B}$ and some $i \in [r]$, and we then have $e_i m' = m' e_i = m$.

◁

Definition 1.8 (quiver, path algebra)**.** A (finite) **quiver** $Q = (Q_0, Q_1, s, t)$ consists of the following data.

- A nonempty finite set Q_0, the **vertices**,
- a nonempty set Q_1, the **arrows**,
- a map $s\colon Q_1 \to Q_0$, the **source**, and
- a map $t\colon Q_1 \to Q_0$, the **target**.

Consider $k\langle Q_0 \dot\cup Q_1\rangle$ as in Example 1.5.1, and consider the compatible ideal $I \subseteq k\langle Q_0 \dot\cup Q_1\rangle$ generated by elements of the form

1. ab,
2. $s(a)a - a$, $at(a) - a$,
3. va, aw,
4. $xx - x$,
5. xy, and
6. $1 - \sum_{u\in Q_0} u$.

where $a, b \in Q_1$ and $v, w, x, y \in Q_0$ such that $s(b) \neq t(a)$, $v \neq s(a)$, $w \neq t(a)$ and $y \neq x$. Then $kQ := k\langle Q_0 \dot\cup Q_1\rangle / I$ is the **path algebra** of the quiver Q. ◁

It is also possible to define a path algebra differently, which can be seen in Definition A.7. That alternative definition requires a bit more work do define it, but once it is defined, we immediately have a grading and a nice multiplicative basis. With the Definition 1.8, we need to do a bit more work to get to these properties. The following proposition allows us to characterize the multiplicative basis that gets inherited from $k\langle Q_0 \dot\cup Q_1\rangle$.

Proposition 1.9. *Let Q be a quiver and define*

$$Q_d = \left\{ \prod_{i=1}^{d} a_i \;\middle|\; \begin{array}{ll} \forall i \in [d]\colon & a_i \in Q_1\ , \\ \forall j \in [d-1]\colon & t(a_j) = s(a_{j+1}) \end{array} \right\} \subseteq k\langle Q_0 \dot\cup Q_1\rangle$$

for $d \geq 2$. Then the Q_d for $d \in \mathbb{N}_0$ are pairwise disjoint, and the projection $\pi\colon k\langle Q_0 \dot\cup Q_1\rangle \twoheadrightarrow kQ$ maps $\bigcup_{d\in\mathbb{N}_0} Q_d$ injectively into kQ. Furthermore, this image is a multiplicative basis of kQ. ◁

Proof (sketch). Let $I \subseteq k\langle Q_0 \dot\cup Q_1\rangle$ be the ideal as defined in Definition 1.8. In $k\langle Q_0 \dot\cup Q_1\rangle$, the Q_d are disjoint in $k\langle Q_0 \dot\cup Q_1\rangle$. What is also immediate by construction, is that none of the Q_d get mapped to 0.

Let $f, g \in \bigcup_{d\in\mathbb{N}_0} Q_d$, such that $f - g \in I$ and assume towards a contradiction that $f \neq g$. Let $\sum_i a_i h_i b_i = f - g$, where $a_i, b_i \in k\langle Q_0 \dot\cup Q_1\rangle$ and h_i are some generators of$I$ as described in Definition 1.8, and assume that there is no redundancy, meaning no partial sum adds up to 0. We will show that $f = \sum_i a_i h_i b_i + g$ will lead to a contradiction. We can always rule out h_i being of the form (6) in Definition 1.8 (we will not show this, this is a bit tricky).

- Case 1: $f \in Q_0$. None of the generators contain a monomial in k, and the only generator that contains a monomial in Q_0 is one of the form (4) in Definition 1.8, so we must have $h_j = ff - f$ and $a_j = -1$, $b_j = 1$ (or similar) for some j, as $f \neq g$ and both are monomials. Since $ff \notin \bigcup_{d\in\mathbb{N}_0} Q_d$ and therefore $g \neq ff$, for $\sum_i a_i h_i b_i + g = f$ to hold, we must cancel out ff without canceling out f, which is not possible, leading to a contradiction.

- Case 2: $f \in Q_1$. Since there are no monomials in k present in any of the generators, we can restrict to looking at generators that contain f, and the only ones that do are the ones of the form (2) in Definition 1.8, so there must be a j such that $h_j = s(f)f - f$ or $h_j = ft(f) - f$ and $a_j = -1$, $b_j = 1$ (or similar). Since there are no other generators that contain a monomial dividing $s(f)f$ or $ft(f)$ and we assumed there to be no redundancy, there is only one h_j corresponding to one of the two proposed generators. Assume that $h_j = s(f)f - f$. But then, since $g \neq s(f)f$ and no other generator contains a monomial that divides $s(f)f$, we cannot cancel out $s(f)f$ in the sum, leading to a contradiction. The case $h_j = ft(f) - f$ is analogous.

- Case 3: $f \in Q_d$ for $d \geq 2$. A generator of the form as described in (1) of Definition 1.8 cannot divide f, as the targets and sources in f are always compatible, via construction of Q_d. The only generators that contain a monomial that divide f are ones of the form $s(c)c - c$ or $ct(c) - c$ for $c \in Q_1$. No matter which $a(s(c)c - c)b$ we choose such that $-acb = f$, there is no way to cancel out $as(c)cb$ without also canceling out $-acb$. Since furthermore $s(a)a$ can't divide g by construction of the Q_k, we have a contradiction.

We have now shown that π maps $\bigcup_{d\in\mathbb{N}_0} Q_d$ injectively into kQ.

Now let us show that $\overline{\bigcup_{d\in\mathbb{N}_0} Q_d}\setminus\{0\} = \overline{\langle Q_0 \dot\cup Q_1\rangle}\setminus\{0, 1\}$. Obviously, $\overline{x} \in \overline{\bigcup_{d\in\mathbb{N}_0} Q_d}\setminus\{0\}$ for $x \in Q_0 \dot\cup Q_1 \subseteq \langle Q_0 \dot\cup Q_1\rangle$ a monomial of degree 1. Let $f = \prod_{i=1}^{e} f_i \in \langle Q_0 \dot\cup Q_1\rangle$ be a monomial of degree $e \geq 2$ such that $\overline{f} \neq 0$. This necessarily implies that for each $j \in [e-1]$, we have (exactly) one of the following cases.

- $f_j, f_{j+1} \in Q_0$ and $f_j = f_{j+1}$,
- $f_j, f_{j+1} \in Q_1$ and $t(f_j) = s(f_{j+1})$,
- $f_j \in Q_1$, $f_{j+1} \in Q_0$ and $t(f_j) = f_{j+1}$, or
- $f_j \in Q_0$, $f_{j+1} \in Q_1$ and $f_j = s(f_{j+1})$.

Now define $f' \in \langle Q_0 \dot\cup Q_1 \rangle$ as the monomial (or word) obtained by removing all symbols of Q_0 occurring in f. Then $f' \in Q_d$ with $d = \#\{i \in [e] \mid f_i \in Q_1\}$, and $\overline{f'} = \overline{f}$, concluding $\overline{\bigcup_{d\in\mathbb{N}_0} Q_d} \setminus \{0\} = \overline{\langle Q_0 \dot\cup Q_1 \rangle} \setminus \{0, 1\}$.

With Proposition 1.4, $\overline{\langle Q_0 \dot\cup Q_1 \rangle} \setminus \{0\}$ is a multiplicative basis of kQ, and therefore with what we just showed, $\overline{\bigcup_{d\in\mathbb{N}_0} Q_d} \setminus \{0\}$ is linearly independent and it is closed under multiplication for nonzero products. Since $1 \in \operatorname{span}_k(\overline{\bigcup_{d\in\mathbb{N}_0} Q_d} \setminus \{0\})$ by (6) in Definition 1.8, we also have that this is a multiplicative basis.

□

Corollary 1.10. *A quiver algebra kQ admits a grading*

$$kQ = \bigoplus_{d\geq 0} (kQ)_d$$

with $(kQ)_d = k\overline{Q_d} = \operatorname{span}_k \overline{Q_d}$. ◁

Definition 1.11 (length)**.** We can write Q_d instead of $\overline{Q_d}$, since we can view $Q_d \subseteq kQ$ for $d \in \mathbb{N}_0$ with Proposition 1.9, and we call an element $a \in Q_d$ a **path of length** d. We also define the map $\ell\colon \bigcup_{d\in\mathbb{N}_0} Q_d \to \mathbb{N}_0$, mapping an element $a \in Q_d$ to its length $\ell(a) = d$.

We furthermore introduce the notation $Q_{\geq n} := \bigcup_{d\geq n} Q_d$ for $n \in \mathbb{N}_0$. ◁

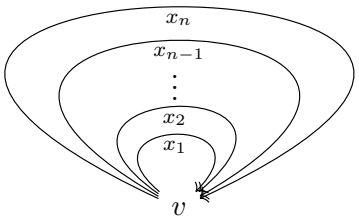
Convention 1.12. If we are given a quiver algebra kQ, then $\mathcal{B} = Q_{\geq 0}$ is the implied multiplicative basis for a quiver algebra. ◁

Definition 1.13. We extend the definition of the source and the target from Q_1 to all of $\bigcup_{d\in\mathbb{N}_0} Q_d$ as follows. For $v \in Q_0$, we define $s(v) = t(v) = v$. For $w \in Q_{\geq 2}$, if we write $w = \prod_{i=1}^{d} w_i$ where $w_i \in Q_1$ and $d = \ell(w)$, we define $s(w) = s(w_1)$ and $t(w) = t(w_d)$. ◁

Remark 1.14. For $u, w \in Q_{\geq 0}$, we have $uw \neq 0$ if and only if $t(u) = s(w)$. In particular, if $u \in Q_{\geq 0}$ and $v \in Q_0$, then $vu = u$ if and only of $s(u) = v$ and we have $uv = u$ if and only if $t(u) = v$, which is an example of Proposition 1.6. ◁

Remark 1.15. The noncommutative polynomial ring in the variables $X = \{x_1, \ldots, x_n\}$ is a special case of a path algebra. It is indeed the path algebra with $Q_0 = \{v\}$ a singleton, which immediately determines s and t, and $Q_1 = X$, and the notions of the length and

degree coincide. We furthermore have $1_{kQ} = v$.



◁

1.2. Admissible orders

Definition 1.16 (order, well order)**.** A **partial order** on a set M is a transitive relation $\preceq$ on M that is antisymmetric, meaning $a = b$ if and only if $a \preceq b$ and $b \preceq a$ for $a, b \in M$. We call $(M, \preceq)$ a partially ordered set, and sometimes just write M when $\preceq$ is implied.

We denote by $\preceq_{\text{rev}}$ the **reverse partial order** of $\preceq$, defined by $a \preceq_{\text{rev}} b :\iff b \preceq a$, and we write $M_{\text{rev}} := (M, \preceq_{\text{rev}})$.

For a partial order $\preceq$, we write $a \prec b$ if $a \preceq b$ and $a \neq b$.

A **partial well order** is a partial order such that every nonempty subset $S \subseteq M$ has a minimal element, meaning an element $m \in S$ such that $a \preceq m$ implies $a = m$ for any $a \in S$.

A **total order** on M is a partial order $\preceq$ such that for all $a, b \in M$ we have $a \preceq b$ or $b \preceq a$. Total orders are sometimes also just referred to as orders.

A **well order** on M is a total order that is also a partial well order. ◁

Remark 1.17. A partial order $\preceq$ is a partial well order if and only if $\prec$ is a well-founded relation. A relation $\sim$ on a set M is called well-founded if the only inductive subset of M is M itself. For a subset $S \subseteq M$, we call S inductive (with respect to $(M, \sim)$) if the following holds for every $x \in M$: *If $y \sim x$ for all $y \in S$, then $x \in S$.* ◁

Proposition 1.18. *Any subset $S \subseteq M$ of a well-ordered set M has a unique minimal element.* ◁

Proof. Let $m, m' \in S$ be two minimal elements. Since we have a total order, we must have $m \preceq m'$ or $m' \preceq m$, and in each of these cases it follows that $m = m'$ by minimality. □

Proposition 1.19. *Let $\preceq$ be a well order on a set M. Then each descending chain in M stabilizes. This means that for a sequence $(m_n)_{n \in \mathbb{N}_0} \in M^{\mathbb{N}_0}$ of elements in M such that $m_n \succeq m_{n+1}$ for all $n \in \mathbb{N}_0$, there exists $d \in \mathbb{N}_0$ such that $m_n = m_d$ for all $n \geq d$.* ◁

Proof. For $S \subseteq M$ the set of all elements that occur in $(m_n)_{n \in \mathbb{N}_0}$, there must exist a minimal element $s \in S$. There then exists $d \in \mathbb{N}_0$ such that $m_d = s$. Let $n \geq d$. By minimality, we must have $m_n \succeq m_d$, but since we have a descending chain, we have $m_n \preceq m_d$, so we have $m_n = m_d$. □

Example 1.20. 1. The vertices V of a cycleless directed graph admit a partial order defined by $v \preceq w$ for $v, w \in V$ if and only if w is reachable from v. This is in general not a total order, even if it is connected.

2. The natural order for the natural numbers is a well order.

3. The natural order on the integers $\mathbb{Z}$ is not a well order, as for instance the whole set itself doesn't contain a minimal element.

4. If we consider $\mathbb{Z}\dot\cup\mathbb{Z}$, we have a partial order defined by $z_1 \prec z_2$ if and only if z_1 is contained in the first (left) copy of $\mathbb{Z}$ and z_2 is contained in the second (right) copy of $\mathbb{Z}$. This is a partial well order.

5. Any total order on a finite set is a well order.

6. If we view a natural number $n \in \mathbb{N}_0$ as a set in its von Neumann construction $n = \{0, \dots, n-1\}$, then the set $\mathbb{N}_0$ is a well-ordered set with the relation $\subseteq$. In the same way, $[n]$ becomes a well-ordered set.

7. The usual order on the interval $[0, \infty) \subseteq \mathbb{R}$ is not a well order, as the subset $(0, \infty)$ has no minimal element.

8. Let $C\colon J \to S$ be a map such that J is totally ordered, and such that $C(j)$ is totally ordered for every $j \in J$. In other words, $(C_j)_{j\in J} = (C(j))_{j\in J}$ is a collection of totally ordered sets indexed by a totally ordered set J. Then $M = \dot\bigcup C = \dot\bigcup_{j\in J} C_j$ is totally ordered: If $c \in C_i$ and $d \in C_j$, then the order $\prec$ on M defined by $c \prec d$ if and only if $i \prec_J j$ or $i = j$ and $c \prec_{C_i} d$ is a total order. If J and each C_j is well-ordered, then M is well-ordered.

◁

Definition 1.21 (lexicographic order)**.** Let A be a well-ordered set and let B be a totally ordered set. We define a total order $\preceq$, the (**left**) **lexicographic order**, on B^A in the following way. Let $f, g \in B^A$, and consider the set $N = \{a \in A \mid f(a) \neq g(a)\} \subseteq A$. If N is nonempty, N has a minimal element $m = \min N$, and we define

$$f \prec g :\iff f(m) \prec_B g(m) .$$

Since every subset of a totally ordered set is also totally ordered, together with Example 1.20.8, we can also define a total order on $\bigtimes C = \bigtimes_{j\in J} C_j \subseteq (\dot\bigcup_{j\in J} C_j)^J$. This is also called the **lexicographic order**.

For finite A and finite J, the reverse orders $A_{\mathrm{rev}} = (A, \preceq_{A,\mathrm{rev}})$ and $J_{\mathrm{rev}} = (J, \preceq_{J,\mathrm{rev}})$ are also well-ordered sets. If we define the lexicographic order with respect to the reverse order of J and A, then we call this the **reverse** (or **right**) **lexicographic order**, which we denote by $\bigtimes_{j\in J_{\mathrm{rev}}} C_j$ and $B^{A_{\mathrm{rev}}}$.

Consider for $n \in \mathbb{N}_{>0}$ the well-ordered set $B^{[n]_{\mathrm{rev}}}$ via the reverse lexicographic order. For $m, n \in \mathbb{N}_0$ with $m \leq n$ we have an embedding $B^{[m]_{\mathrm{rev}}} \hookrightarrow B^{[n]_{\mathrm{rev}}}$ by appending $n - m$ entries of the minimal element $\min(B)$ in B to the end of the sequence. This diagram has

a colimit, whose underlying set we will call $\mathrm{fseq}(B)$, the finite sequences with values in B. The order resulting from taking this colimit is called the **reverse** (or **right**) **length lexicographic order** on $\mathrm{fseq}(B)$.

It is also possible to completely analogously define the reverse length lexicographic order for indices in $\mathbb{N}_0$ instead of $\mathbb{N}_{>0}$. ◁

Remark 1.22.

1. The lexicographic order for B^A and for $C^{\times J}$ are indeed well-defined total orders, but each not necessarily well orders, even if B and every C_j are also well-ordered. If A and C_j are finite, we do in fact have a well-order in both cases.

2. If B is a well-ordered set, the reverse length lexicographic order on the finite sequences $\mathrm{fseq}(B)$ is well-ordered.

3. The set $\mathrm{fseq}(B)$ is in bijection with the set of all sequences $a \in B^{\mathbb{N}_{>0}}$ such that there exists $d \in \mathbb{N}_{>0}$ with $a_n = \min(B)$ for all $n \geq d$.

4. If α and β are ordinal numbers, then the ordinal number $\alpha + \beta$ defined via ordinal arithmetic corresponds to $A \dot{\cup} B$ in our construction, if A and B are the well-ordered sets corresponding to α and β, respectively.

5. If α is an ordinal number and ω is the ordinal number corresponding to $\mathbb{N}_0$, then α^ω defined via ordinal arithmetic corresponds to the reverse length lexicographic order on $\mathrm{fseq}(B)$, if B is the underlying well-ordered set.

◁

Example 1.23.

1. For $[3] \times [5] = \bigtimes_{i \in [2]} C_i$ with $C_1 = [3]$ and $C_2 = [5]$, we have

$$\begin{aligned}(1,1) &\prec (1,2) \prec (1,3) \prec (1,4) \prec (1,5)\\ &\prec (2,1) \prec (2,2) \prec (2,3) \prec (2,4) \prec (2,5)\\ &\prec (3,1) \prec (3,2) \prec (3,3) \prec (3,4) \prec (3,5)\ .\end{aligned}$$

   Note that it is indeed important to specify what well-ordered index set we take the Cartesian product over, as the definition of the lexicographic order depends on it. Implicitly, the written down order of the sets occurring in the expression $[3] \times [5]$ can also dictate this, meaning the set on the left, $[3]$, is regarded as being "first", and set on the right, $[5]$, is regarded as being "second".

2. The sets $\mathbb{N}_0^{[2]}$ and $\mathbb{N}_0 \times \mathbb{N}_0 = \bigtimes_{i \in [2]} C_i$ with $C_1 = C_2 = \mathbb{N}_0$ can be identified with each other in the usual way, and both constructions of the lexicographic order in Definition 1.21 lead to the same order.

$$\begin{aligned}(1,1) &\prec (1,2) \prec (1,3) \prec \cdots\\ &\prec (2,1) \prec (2,2) \prec (2,3) \prec \cdots\\ &\prec (3,1) \prec (3,2) \prec (3,3) \prec \cdots\\ &\ \ \vdots\end{aligned}$$

3. The lexicographic order for $\{1,0\}^{[8]}$ corresponds to the order of the binary representation of the numbers between 0 and 255 with leading zeroes, just like a byte of data in a computer. This also works for any b-ary number system with $B = \{b-1, b-2, \dots, 1, 0\}$ and larger exponents.

4. For $B = \{9, 8, \dots, 1, 0\}$, the lexicographic order on $B^{\mathbb{N}_{>0}}$ almost exactly corresponds to the order for the decimal representation of real numbers between 0 and 1, except for the edge cases where the sequence has repeating 9's after a certain index. For example, $0.1\overline{9} = 0.2$, but we have $19999\ldots \prec 20000\ldots$ for the corresponding sequences in $B^{\mathbb{N}_{>0}}$.

   We also see how this is not a well order, since

   $$1000\ldots \succ 0100\ldots \succ 0010\ldots \succ \cdots ,$$

   or in more familiar terms, $0.1 > 0.01 > 0.001 > \cdots$, is a nonstabilizing descending sequence.

5. Consider $\mathrm{fseq}(\{9, 8\ldots, 1, 0\})$, ordered with the reverse lexicographic order.

   Let $x, y \in \mathrm{fseq}(\{9, \dots, 0\})$, and consider these as sequences as described in Remark 1.22.3, meaning there exist minimal $d, e \in \mathbb{N}_{>0}$ such that $x_n = 0$ for all $n \geq d$ and $y_n = 0$ for all $n \geq e$. Then there are elements $x' \in B^{[d]_{\mathrm{rev}}}$ and $y' \in B^{[e]_{\mathrm{rev}}}$ that correspond to x and y in the colimit. We then have

   $$x \prec y \iff \begin{cases} d < e \quad \text{or} \\ d = e \text{ and } x'_j < y'_j \text{ for } j = \max\{i \in [d] \mid x'_i \neq y'_i\} \end{cases} .$$

   This example illustrates how the decimal representation of the natural numbers are ordered, but we must think of the sequence of digits to start on the right and go to the left.

   Interestingly, this is how one thinks about numbers in Arabic, which is where the decimal numbers of the Western world come from. Here, the digits of a number appear in the same way, but in the written language of Arabic, one reads from right to left. This is also in line with the exponents of the b-adic representation of natural numbers, we write $x = \sum_{n \in \mathbb{N}_{>0}} x_n b^{n-1}$, where $x_n \in \{b-1, b-2\ldots, 1, 0\}$ (in our case $b = 10$) and there exists $d \in \mathbb{N}_{>0}$ such that $x_n = 0$ for all $n \geq d$.

   A number like $x = 69$ then has the "first" digit $x_1 = 9$ and the "second" digit $x_2 = 6$. This number can also be written as 069 or 0069 etc., or the sequence $\ldots 0000069$. In the above characterization of the reverse length lexicographic order, x' and y' are representatives such that they have no "trailing zeroes", and d and e can be thought of as the **length** of a and b. In the case of the decimal representation of natural numbers, this terminology might be confusing, because the trailing zeroes are on the left. We could also instead say "without leading zeroes", but this is also confusing since we said that the "first" digit is on the right.

Let us compare the decimal representations $x = \ldots 000069$ and $y = \ldots 000420$. We then have $x' = 69$ and $y' = 420$, and see $d = 2$ and $e = 3$, therefore $x \prec y$.

For a different example, let $x = \ldots 00012359$, and $y = \ldots 0012409$, so $x' = 12359$ and $y' = 12409$. We have $d = e = 5$, so then we check $j = \max\{i \in [d] \,|\, x'_i \neq y'_i\} = 3$ and see $x_3 < y_3$, therefore $x \prec y$. In other words, in the left most digit of where x and y differ, that digit in x is smaller than that digit in y.

We have now seen that we have a bijection $\mathbb{N}_0 \leftrightarrow \mathrm{fseq}(\{9, \ldots, 0\})$ that preserves the order, and so we can convince ourselves that the reverse length lexicographic order is a well order, since $\mathbb{N}_0$ is well-ordered.

◁

Remark 1.24 (An excursion on the arithmetic of ordinals)**.** The definition of the exponentiation for ordinal numbers might at first seem like it wouldn't translate to greater ordinals, as we can't reverse the order of transfinite ordinals to receive a transfinite ordinal, but indeed it actually works. The underlying mechanism responsible for the quirk that "the order of the indices is reversed" is that in the definition for arithmetic on ordinals, addition and multiplication are based on transfinite induction on the second argument, multiplication is based on the distributive law on the left, and the exponentiation is based on expansion on the left. The aforementioned properties are formally the following formulas.

- $\alpha + \mathrm{succ}(\beta) = \mathrm{succ}(\alpha + \beta)$
- $\alpha \cdot \mathrm{succ}(\beta) = \alpha \cdot \beta + \alpha$
- $\alpha^{\mathrm{succ}(\beta)} = \alpha^\beta \cdot \alpha$

Working everything out, for an ordinal number $\alpha > 1$, we have $\alpha^2 = \alpha \cdot \alpha$ and $\alpha = \alpha \cdot 1 < \alpha \cdot \alpha$. This means $\alpha \in \alpha \cdot \alpha$, so we have $\alpha \subseteq \alpha \cdot \alpha$ (actually "$\subsetneq$"), and the elements in α are the "smallest α many elements" in $\alpha \cdot \alpha$. In terms of well ordered sets, say A is the canonical von Neumann representative of α, we have $\alpha \cong \alpha \times \{0\} \subseteq \alpha \times \alpha$. All together, we have that any $(a, 0) \in A \times A$ is smaller then any $(a, a') \in A \times A$ for $a' > 0$. Recursively, we can see that we have $A \times A$ is ordered according to $A^{2_{\mathrm{rev}}}$, the reverse (or right) lexicographic order. ◁

Definition 1.25 (admissible order)**.** Let A be a k-algebra with multiplicative basis $\mathcal{B}$. We call a well order $\prec$ on $\mathcal{B}$ an **admissible order** if the following conditions hold for all $p, q, r, s \in \mathcal{B}$.

(O1a) $pr \neq 0,\ qr \neq 0,\ p \preceq q \implies pr \preceq qr$

(O1b) $sp \neq 0,\ sq \neq 0,\ p \preceq q \implies sp \preceq sq$

(O2) $p = qr \implies q \preceq p,\ r \preceq p$

◁

Remark 1.26. For $b, c, d \in \mathcal{B}$ we have

$$b \preceq bc \quad \text{and} \quad b \preceq db\,,$$

as in each case we have $bc \in \mathcal{B}$ and $db \in \mathcal{B}$, respectively, and can apply (O2) to $q = b$, $r = c$, and $p = bc$, and to $q = d$, $r = b$, and $p = db$, respectively. ◁

Proposition 1.27. *Let A be a k-algebra with multiplicative basis $\mathcal{B}$ and an admissible order $\preceq$, and let $I \subseteq A$ be a monomial ideal. Then the order $\preceq'$ defined by*

$$\overline{b} \preceq' \overline{c} :\iff b \preceq c$$

for $\overline{b}, \overline{c} \neq 0$ is a well-defined admissible order on $\overline{\mathcal{B}} \setminus \{0\} \subseteq A/I$. ◁

Proof. Since I is a monomial ideal, with Proposition 1.4, $\overline{\mathcal{B}} \setminus \{0\}$ can be identified with $\mathcal{B} \setminus I$, and we see that the order $\preceq'$ on $\overline{\mathcal{B}}$ is the same as the restriction of $\preceq$ to $\mathcal{B} \setminus I$, so $\preceq'$ is a well-defined well order. It is also an admissible order, because $\overline{a} \cdot \overline{b} \neq 0$ implies $a \cdot b \neq 0$, and then the axioms (O1a), (O1b), and (O2) transfer from A to A/I. □

Definition 1.28 (lexicographic order)**.** Let $Q = (Q_0, Q_1, s, t)$ be a quiver, and assume that we have equipped Q_0 and Q_1 each with well orders, such that $Q_{\leq 1} = Q_0 \cup Q_1$ is then also well-ordered, as described in Definition 1.21.

Any element $a \in Q_{\geq 0}$, say $a \in Q_d$, can be uniquely assigned a sequence $\tilde{a} \in (Q_{\leq 1})^{\mathbb{N}_{>0}}$ such that for all $i \in [d]$ we have $\tilde{a}(i) \in Q_1$ and for all $r > d$ we have $\prod_{i=1}^{r} \tilde{a}(i) = a$. This necessarily implies that $\tilde{a}(i) = t(\tilde{a}(d)) = t(a) =: t$ for all $i > d$. We write $a_i = \tilde{a}(i)$, and can by abuse of notation say

$$a = a_1 a_2 a_3 \dots a_{d-1} a_d t t t t t \dots\,.$$

What was done here can be seen as artificially extending a path such that when we do comparisons between paths, we need not worry about their length being unequal.

With this assignment, we have formed an inclusion $Q_{\geq 0} \subseteq (Q_{\leq 1})^{\mathbb{N}_{>0}}$. The **left lexicographic order** $\preceq_{\texttt{Lex}}$ on $Q_{\geq 0}$ is then the restriction of the left lexicographic order $\preceq$ of $(Q_{\leq 1})^{\mathbb{N}_{>0}}$ as described in Definition 1.21.

Consider the quiver algebra of $Q' = (Q_0, Q_1, t, s)$, which is just Q with reversed arrows. kQ and kQ' are isomorphic as k-algebras by reversing the path. Specifically, the isomorphism sends $v \mapsto v' := v$ for $v \in Q_0$ and $a \mapsto a' := a_d \dots a_1$ for $a \in Q_{\geq 1}$. We define the **right lexicographic order** (`lex`) by

$$a' \preceq_{\texttt{lex}} b' :\iff a \preceq_{\texttt{Lex}} b\,.$$

◁

Convention 1.29. When the elements of a set X are given a list of elements, it is usually implied that they are listed in descending order. This means that if we for instance write $X = \{x, y, z\}$, we imply the well order $x \succ y \succ z$.

◁

Remark 1.30.

- If $X = \{x_1, x_2, \dots, x_n\}$ is an enumerated set, we have, perhaps confusingly, the implied order $x_i \preceq x_j \iff i \geq j$.
- Let $X = \{a, b, c, \dots, x, y, z\}$ (the alphabet) with the implied ordering

$$a \succ b \succ c \succ \cdots \succ x \succ y \succ z \,.$$

  Then "words" in the colloquial sense are words in our sense (non-commutative monomials) in X. Let us consider consider `Lex`. If we arrange words in descending order, the sequence would start with the longest words that start with the letter a, and end with the shortest words that start with the letter z, which differs from the sequence of words in a colloquial dictionary from front to back, which start with the shortest words. If we take the subset of words of length d, then the words do appear in the same order as in a colloquial dictionary.
- If we wanted to construct a scenario where an ordering would amount to the ordering in a colloquial dictionary, we would start with $X = \{z, y, x, \dots, c, b, a\}$ (the alphabet), and order them as $z \succ \cdots \succ a$. Then, if we put words in the sequence of ascending order with respect to `Lex`, it would be the same as taking the sequence of words in a colloquial dictionary from front to back.

◁

Remark 1.31. The left and right lexicographic orders are well orders, but **not** admissible orders on path algebras. As an example, if we again consider $k\langle X\rangle$ and take $X = \{x, y, z\}$ with $x \succ y \succ z$, then $x \prec_{\texttt{Lex}} xz$, but $x \cdot y \succ_{\texttt{Lex}} xz \cdot y$ violating (O1a). ◁

Definition 1.32 (weight extension)**.** Let $\mathcal{B}$ be a multiplicative basis for a k-algebra A, and let $\preceq$ be a well order. Let $\alpha\colon \mathcal{B} \to \mathbb{N}_0$ be a **weight** function, meaning a map such that for all $b, b' \in \mathcal{B}$ with $b \cdot b' \neq 0$ we have $\alpha(b \cdot b') = \alpha(b) + \alpha(b')$. We then define a new order $\preceq_\alpha$ on $\mathcal{B}$ as follows.

We can partition our multiplicative basis into subsets $\mathcal{B} = \bigcup_{d\in\mathbb{N}_0} \mathcal{B}_d$, where $\mathcal{B}_d := \{b \in \mathcal{B} \mid \alpha(b) = d\}$ are the basis elements of weight d. Each $\mathcal{B}_d \subseteq \mathcal{B}$ is well-ordered via $\preceq$. Our new order $\preceq_\alpha$ on $\mathcal{B} = \bigcup_{d\in\mathbb{N}_0} \mathcal{B}_d$, the **weight extension** of $\preceq$ by α, is then the one resulting from the construction (8) in Example 1.20.

(Compare to [Dec+21, Chapter 7.9.2].)

◁

Definition 1.33 (weighted lexicographic order)**.** In the case of a path algebras, the weight function α is uniquely determined by its **weight vector** $\texttt{v} = \alpha|_{Q_1} \in \mathbb{N}_0^{Q_1}$. We write `(a(v),o)` for the weight extension of the total order `o` by the weight vector `v`. For the special cases of `o` = `Lex` and `o` = `lex`, we write `Wp(v)` and `wp(v)`, respectively, called the **weighted left** (resp. **right**) **lexicographic order**. If $\texttt{v} = (1, \dots, 1)$, we write `Dp` = `Wp(v)` and `dp` = `wp(v)`, called the **left**, resp. **right** (or **reverse**) **length lexicographic order** or **degree lexicographic order**. ◁

Remark 1.34. Let Q be a quiver and kQ its path algebra. Each element in $a \in Q_{\geq 0}$, say with $\ell(a) = d$ can be uniquely assigned a sequence $\tilde{a} \in Q_{\leq 1}^{d+1}$ such that

$a = \prod_{i=0}^{d} \tilde{a}(i)$, where $\tilde{a}(i) \in Q_1$ for $i \in [d]$ and $a_0 = s(a)$. We have now formed an inclusion $Q_{\geq 0} \subseteq \mathrm{fseq}(Q_{\leq 1})$. The reverse (or right) length lexicographic order on $\mathrm{fseq}(Q_{\leq 1})$ as in Definition 1.21 restricted to $Q_{\geq 0}$ then coincides with the right length lexicographic order as in Definition 1.32. ◁

Proposition 1.35. *Let Q be a quiver. If $\mathtt{v} \in (\mathbb{N}_{>0})^{Q_1}$ is a strictly positive weight vector, then $\preceq_{\mathtt{Wp(v)}} = \preceq_{\mathtt{(a(v),Lex)}}$ and $\preceq_{\mathtt{wp(v)}} = \preceq_{\mathtt{(a(v),lex)}}$ are admissible orders on kQ, in particular $\preceq_{\mathtt{Dp}}$ and $\preceq_{\mathtt{dp}}$. If $\mathtt{v} \in \mathbb{N}_0^{Q_1}$ is any weight vector, then $\preceq_{\mathtt{(a(v),o)}}$ is an admissible order kQ for any admissible order $\mathtt{o}$.* ◁

Proof (sketch). Consider $\preceq := \preceq_{\mathtt{Wp(v)}}$ for a strictly positive weight vector $\mathtt{v}$. For (O2), it suffices to know that $p = qr$ implies both $w(p) \geq w(q)$ and $w(p) \geq w(r)$, and that $q \preceq_{\mathtt{Lex}} p$ and $r \preceq_{\mathtt{Lex}} p$. It is apparent that for $p, q, s \in Q_{\geq 0}$ with $sp \neq 0$ and $sq \neq 0$, we have that $p \preceq_{\mathtt{Lex}} q$ implies $sp \preceq_{\mathtt{Lex}} sq$, because `Lex` "checks from left to right", and both paths start with the same subpath s. This implies (O1b), since this covers the case where $w(p) = w(q)$ and therefore $w(sp) = w(sr)$. Now let $p, q, r \in Q_{\geq 0}$ such that $pr \neq 0$, $qr \neq 0$ and assume $p \preceq q$. If $w(p) < w(q)$, then clearly $w(pr) = w(p) + w(r) < w(q) + w(r) = w(qr)$, so $pr \prec qr$.

Now assume $w(p) = w(q)$, in which case we must then have $p \preceq_{\mathtt{Lex}} q$. This means that $w(pr) = w(qr)$, so we must now show that $pr \preceq_{\mathtt{Lex}} qr$. Assume towards a contradiction that $pr \succ_{\mathtt{Lex}} qr$. This means that we initially must have had $p \neq q$, so $p \prec_{\mathtt{Lex}} q$. The only way that $p \prec_{\mathtt{Lex}} q$ can be true while $pr \succ_{\mathtt{Lex}} qr$, is if p is a subpath of q, more specifically q must be of the form $q = ps$ for some nonempty path s. But if $\mathtt{v}$ is a nonzero weight vector, then $w(p) < w(p) + w(s) = w(q)$, so $w(pr) = w(p) + w(r) < w(q) + w(r) = w(qr)$, which means that $pr \prec qr$, which is a contradiction.

The case for `wp(v)` is completely analogous (or can be proven by applying the case for `Wp(v)` to kQ', the path algebra with reversed arrows).

□

Example 1.36.

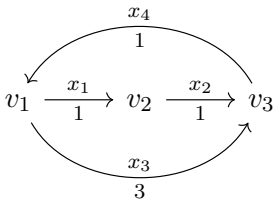
- Consider $k\langle x, y, z\rangle$ with $x \succ y \succ z$. We then have

$$\begin{aligned} & 1 && \text{degree } 0 \\ \prec_{\mathtt{Dp}}\ & z \prec_{\mathtt{Dp}}\ y \prec_{\mathtt{Dp}}\ x && \text{degree } 1 \\ \prec_{\mathtt{Dp}}\ & z^2 \prec_{\mathtt{Dp}} zy \prec_{\mathtt{Dp}} zx \prec_{\mathtt{Dp}} yz \prec_{\mathtt{Dp}} y^2 \prec_{\mathtt{Dp}} yx \prec_{\mathtt{Dp}} xz \prec_{\mathtt{Dp}} xy \prec_{\mathtt{Dp}} x^2\,, && \text{degree } 2 \end{aligned}$$

  and we have

$$\begin{aligned} & 1 && \text{length } 0 \\ \prec_{\mathtt{dp}}\ & z \prec_{\mathtt{dp}}\ y \prec_{\mathtt{dp}}\ x && \text{length } 1 \\ \prec_{\mathtt{dp}}\ & z^2 \prec_{\mathtt{dp}} yz \prec_{\mathtt{dp}} xz \prec_{\mathtt{dp}} zy \prec_{\mathtt{dp}} y^2 \prec_{\mathtt{dp}} xy \prec_{\mathtt{dp}} zx \prec_{\mathtt{dp}} yx \prec_{\mathtt{dp}} x^2\,. && \text{length } 2 \end{aligned}$$

- Consider the quiver algebra kQ for the following quiver.



  Let `Lex` be the lexicographic ordering for $x_1 \succ x_2 \succ x_3 \succ x_4$ for and $v_1 \succ v_2 \succ v_3$. Let furthermore w be the weight defined by the weight vector $(1, 1, 4, 1)$, meaning $w(x_1) = 1$, $w(x_2) = 1$, $x_3 = 3$, and $w(x_4) = 1$, and consider $\preceq := \preceq_{\texttt{(Wp(w),Lex)}}$, the weight extension of `Lex` by w. We then have

$$\begin{array}{rrrrrrrrrrrrr}
 & & & & & & v_3 & \prec & v_2 & \prec & v_1 & & & & \text{weight } 0 \\
\prec & & x_4 & \prec & & & x_2 & \prec & & & x_1 & & & & \text{weight } 1 \\
\prec & & x_4x_1 & \prec & & & x_2x_4 & \prec & & & x_1x_2 & & & & \text{weight } 2 \\
\prec & x_4x_1x_2 & & \prec & & & x_3 & \prec & x_2x_4x_1 & \prec & & & x_1x_2x_4 & & \text{weight } 3 \\
\prec & & x_4x_3 & \prec & & & x_2x_3 & & & & & & & & \text{weight } 4 \\
\prec & x_3x_4x_1 & & \prec & x_2x_4x_3 & . & & & & & & & & & \text{weight } 5
\end{array}$$

  $\lhd$

We now briefly discuss orders for the commutative polynomial ring, similar to how it is discussed in [Mor94, p. 133].

Definition 1.37. Assume that a total order is given on the finite set X, so without loss of generality $X = \{x_1, \dots, x_n\}$ and $x_1 \succ \dots \succ x_n$. Then we can write each $b \in [X]$ (uniquely) as $\prod_{i=1}^n x_i^{\alpha_i}$ for some $\alpha \in \mathbb{N}_0^{[n]}$. We now define an inclusion of vector spaces $\Delta\colon k[X] \to k\langle X\rangle$ by the linear extension of $\prod_{i=1}^n x_i^{\alpha_i} \mapsto \prod_{i=1}^n x_i^{\alpha_i} = x_1^{\alpha_1} \dots x_n^{\alpha_n}$. $\lhd$

For our previously defined admissible orders, we can define an admissible order for $k[X]$ by this inclusion.

Definition 1.38. For an order $\preceq_o$, with o being either `Wp(w)`, `wp(w)` (in particular `Dp` and `dp`), `Lex`, `lex`, `(a(v),Dp)`, or `(a(v),dp)`, we define

$$b \preceq_o b' :\iff \Delta(b) \preceq_o \Delta(b')$$

for elements in our multiplicative basis $b, b' \in [X] \subseteq k[X]$. $\lhd$

Proposition 1.39. *Definition 1.38 defines an admissible order for* `w` *strictly positive.* $\lhd$

Proof. Property (O2) is apparent, as the argument here is purely weight based. We now want to prove (O1). Let $u, u', v \in [X]$, say $u = \prod_{i=1} nx^{\alpha_i}$, $u' = \prod_{i=1} nx^{\beta_i}$ and $v = \prod_{i=1} nx^{\gamma_i}$, let $x_j \in X$ for some $j \in [n]$, and Assume that $u \preceq v$. If $\ell(u) \prec \ell(v)$, the argument is again purely weight based, so $ux_j \preceq vx_j$. If $\ell(u) = \ell(v)$, let $s \in [n]$ be the (unique) index such that $\alpha_s < \beta_s$ and $\forall i < s\colon \alpha_i = \beta_i$. We then get $\alpha_s + \gamma_s < \beta_s + \gamma_s$ and $\alpha_i + \gamma_i = \beta_i + \gamma_i$ for all $i < s$, and therefore $uv \preceq u'v$. $\square$

Remark 1.40. The orders `Lex` and `lex` are in general not admissible orders for path algebras, as noted in Remark 1.31, but for the commutative case, they are. ◁

1.3. Noncommutative polynomials in Singular

Let us return to our example in Example 1.5.3, but let us now make it more concrete with $X = \{x, y, z\}$ and $d = 6$. This means that we have the algebra $A = k\langle x, y, z\rangle$ with multiplicative basis $\mathcal{B} = \langle x, y, z\rangle$ and the monomial ideal $I = (M) \subseteq A$ generated by $M = \{m \in \langle X\rangle \mid \ell(m) > d\} \subseteq \mathcal{B}$, giving us $A/I = k\langle X\rangle_{\leq 6}$, the ring of polynomials of degree at most 7. Let us choose $\preceq_{\texttt{Dp}}$ as our admissible order for $k\langle x, y, z\rangle$. Then $k\langle X\rangle_{\leq 6}$ also has admissible order $\preceq_{\texttt{Dp}}$ by Proposition 1.27.

Let us see how we can define this in SINGULAR ([Dec+21]). We first load the `freegb` library. Then we initialize a commutative polynomial ring in the variables `x`, `y` and `z`, with order `Dp`. Then with this data, we define our ring $\texttt{A} = k\langle x, y, z\rangle_{\leq 6}$ and set it.

```
> LIB "freegb.lib";
> ring R = 0,(x,y,z),Dp;
> def A = freeAlgebra(R,6);
> setring A;
> A;

// coefficients: QQ
// number of vars : 18
//        block   1 : ordering Dp
//                  : names    x y z x y z x y z x y z x y z x y z
//        block   2 : ordering C
// letterplace ring (block size 3, ncgen count 0)
```

In SINGULAR, we first start by defining the commutative polynomial ring before we define our noncommutative polynomial ring. SINGULAR lets us use the orderings `Dp`, `dp`, `Wp(w)`, `wp(w)`, `lp`, `rp` and `(a(v),o)`. The implementation of a noncommutative polynomial ring in SINGULAR is actually done in terms of commutative polynomials, and such rings are called **letterplace rings**. This concept was introduced in [LL09], and is described further in [Zei19, Chapter 4]. Let us briefly outline what is happening.

Assume we want to model $k\langle x_1, \ldots, x_n\rangle_{\leq d}$. We introduce the polynomial ring in $m \cdot d$ variables, the variables of which we shall name $x_{i,j}$ for $i \in [n]$ and $j \in [d]$. If we have a monomial $\prod_{k=1}^{e} x_{i_k} \in k\langle x_1, \ldots, x_n\rangle_{\leq d}$ with $e \leq d$, the corresponding commutative polynomial then is $\prod_{k=1}^{e} x_{i_k,k} \in k[x_{1,1}, \ldots, x_{n,d}]$. The intuition behind this is that the second index encodes the position of the variable, that is $x_{i,j}$ stands for "x_i at the j-th position". For this reason, SINGULAR lists 18 variables for our ring `A`. This way the order of the $x_{i,j}$ doesn't matter to encode the information of the non-commutative monomial. The tricky part is where we perform operations in $k[x_{1,1}, \ldots, x_{n,d}]$ while still trying to make statements in our original polynomial ring $k\langle x_1, \ldots, x_n\rangle$. The aforementioned map, call it $\Phi\colon k\langle x_1, \ldots, x_n\rangle_{\leq d} \to k[x_{1,1}, \ldots, x_{n,d}]$, is an embedding of k-vector spaces, but it

is not surjective, as for instance any monomial that contains two variables x_{i_1,j_1} and x_{i_2,j_2} with $j_1 = j_2$ in its expression doesn't have a corresponding monomial in $k\langle x_1, \ldots, x_n\rangle_{\leq d}$.

The map Φ is not compatible with the multiplication: For $m \cdot m' \in k\langle x_1, \ldots, x_n\rangle_{\leq d}$, we in general have $\Phi(m \cdot m') \neq \Phi(m) \cdot \Phi(m') \in k[x_{1,1}, \ldots, x_{n,d}]$, so we need to consider an alternate multiplication in $k[x_{1,1}, \ldots, x_{n,d}]$, where we must "shift" the variables. We therefore define

$$(\prod_{k=1}^{e} x_{i_k,k}) \odot (\prod_{k=1}^{e'} x_{i'_k,k}) := (\prod_{k=1}^{e} x_{i_k,k}) \cdot (\prod_{k=1}^{e'} x_{i'_k,e+k})$$

for $e + e' \leq d$.

For orders `Wp(w)` as in Definition 1.33, where $x_1 \succ \cdots \succ x_n$, we choose the order on $\{x_{1,1}, \ldots, x_{n,d}\}$ to be

$$x_{1,1} \succ x_{2,1} \succ \cdots \succ x_{n,1} \succ x_{1,2} \succ x_{2,2} \succ \cdots \succ x_{n,d-1} \succ x_{n,d} \ .$$

If we are given an ordering `Wp(w)` on $k\langle x_1, \ldots, x_n\rangle_{\leq d}$ for a weight vector $w \in \mathbb{N}_{>0}^{[n]}$, consider the weight vector that just copies the weights onto all copies of the x_i, meaning $w' \in \mathbb{N}_{>0}^{[n]\times[d]}$ is defined by $w'_{i,j} := w_i$. We then have

$$u \preceq_{\texttt{Wp(w)}} v \iff \Phi(u) \preceq_{\texttt{Wp(w')}} \Phi(v) \ .$$

Staying in our example of $n = 3$ and $d = 6$, if we want to write down a polynomial in the letterplace ring corresponding to $A = k\langle x, y, z\rangle_{\leq 6}$ in SINGULAR, we have to write an asterisk `*` between all variables. Every outputted polynomial entered will have its terms in descending order.

```
> def a = 7x*y - 2x*y + 4z*x + x*y*z - y*z + 3y*x*z - 2y*z*x;
> a;

x*y*z+3*y*x*z-2*y*z*x+5*x*y-y*z+4*z*x
```

Let us define some other polynomials and perform some operations.

```
> def b = z*z*x + 2z*x;
> def c = 3x*y*x*z*z;
> a*b;

x*y*z*z*z*x+3*y*x*z*z*z*x-2*y*z*x*z*z*x+7*x*y*z*z*x+6*y*x*z*z*x
-4*y*z*x*z*x-y*z*z*z*x+4*z*x*z*z*x+10*x*y*z*x-2*y*z*z*x+8*z*x*z*x

> a+b;

x*y*z+3*y*x*z-2*y*z*x+z*z*x+5*x*y-y*z+6*z*x

> a*c;
```

```
   ? degree bound of Letterplace ring is 6, but at least 8
is needed for this multiplication
   ? degree bound of Letterplace ring is 6, but at least 7
is needed for this multiplication
   ? error occurred in or before STDIN line 37: `b*c;`
```

Multiplications where the resulting polynomial would have degree higher than 6 will result in an error. It is therefore *not* the case that the multiplication works as in $k\langle x, y, z\rangle/\{m \in \langle x, y, z\rangle \mid \deg m > d\}$.

1.4. Gröbner bases

Having discussed admissible orders, we are now finally able to define what a Gröbner basis is. In this section, A will denote a k-algebra with multiplicative basis $\mathcal{B}$ and an admissible order $\preceq$.

Definition 1.41 (leading term)**.** Let $0 \neq y \in A$, which we can write uniquely as

$$\begin{aligned} y &= \sum_{i=1}^{s} \lambda_i b_i \,, && \text{where } \lambda_i \in k^\times \text{ with } b_i \text{ pairwise distinct, and} \\ b_i &\succ b_{i+1} && \text{(descending order)} \end{aligned}$$

for all $i \in [s-1]$. Let furthermore $M \subseteq R$ be a set. We then define

- $\mathrm{LT}(y) := b_1$, the **leading term**,
- $\mathrm{LC}(y) := \lambda_1$, the **leading coefficient**,
- $\mathrm{LM}(y) := \mathrm{LC}(y)\,\mathrm{LT}(y) = \lambda_1 b_1$,
- $\mathrm{LT}\{M\} := \{\mathrm{LT}(f) \mid 0 \neq f \in M\}$, the **leading term set**,
- $\mathrm{LT}(M) = (\mathrm{LT}\{M\})$, the **leading term ideal** of M, and
- $\mathrm{supp}(y) = \{b_i \mid i \in [s]\}$, the **support** of y.

If $\mathrm{LC}(y) = \lambda_1 = 1$, we call y **monic**, and if the set M consists of only monic elements, we call M monic.

◁

Remark 1.42. The leading term ideal $\mathrm{LT}(M)$ for a set $M \subseteq \mathcal{B}$ is a monomial ideal, and we have $\mathrm{LT}(M) = \mathrm{span}_k(\mathrm{LT}\{I\})$ for $I = (M)$ the ideal generated by M. ◁

Proposition 1.43. *Let A be a k-algebra with multiplicative basis $\mathcal{B}$ equipped with a well order. For $f, g \in A$ such that $\mathrm{LT}(f) \cdot \mathrm{LT}(g) \neq 0$ we have $\mathrm{LT}(fg) = \mathrm{LT}(f) \cdot \mathrm{LT}(g)$.* ◁

Proof. This is just a direct result of (O1). If we multiply $f \cdot g$ for $f = \sum_{i=1}^{r} \lambda_i b_i$ and $g = \sum_{j=1}^{s} \mu_i b'_j$, with the b_i and b'_j in descending order, then $\mathrm{LT}(f) \cdot \mathrm{LT}(g) = b_1 \cdot b'_1 \succeq b_i \cdot b'_j$ for all i, j by (O1a) and (O1b). Since $\operatorname{supp} fg \subseteq \{b_i b'_j \mid i \in [r],\, j \in [s]\}$, we have $\mathrm{LT}(fg) = \mathrm{LT}(f) \cdot \mathrm{LT}(g)$. □

Definition 1.44 (Gröbner basis)**.** Let $I \subseteq A$ be an ideal. We call a subset $G \subseteq I$ a **Gröbner basis** of I if

$$(G) = I \quad \text{and} \quad \mathrm{LT}(G) = \mathrm{LT}(I)\ .$$

If G is additionally fulfills

1. $\mathrm{LT}\{G\}$ is a minimal generating set of $\mathrm{LT}(G)$, and
2. $g - \mathrm{LM}(g) \in \operatorname{span}(\mathcal{B} \setminus \mathrm{LT}\{I\})$ for all $g \in G$,

we call G a **reduced Gröbner basis**. ◁

Proposition 1.45. *Let $G \subseteq I$ be a subset of an ideal I. Then G is a Gröbner basis of I if and only if the semigroup in $\mathcal{B}_0$ generated by $\mathrm{LT}\{G\}$ is equal to $\mathrm{LT}\{I\} \cup \{0\}$, in other words $(\mathcal{B} \cdot \mathrm{LT}\{G\} \cdot \mathcal{B}) \setminus \{0\} = \mathrm{LT}\{I\}$ (for every $f \in I \neq \{0\}$ there exists $g \in G$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(f)$).* ◁

Proof. We first notice that $\mathrm{LT}(G) = \mathrm{LT}(I)$ if and only if $(\mathcal{B} \cdot \mathrm{LT}\{G\} \cdot \mathcal{B}) \setminus \{0\} = \mathrm{LT}\{I\}$. This means that we immediately have " $\Longrightarrow$ ", and for " $\Longleftarrow$ ", what is left to show is that $(\mathcal{B} \cdot \mathrm{LT}\{G\} \cdot \mathcal{B}) \setminus \{0\} = \mathrm{LT}\{I\}$ implies $(G) = I$.

We prove this by contraposition. Let $(G) \subsetneq I$. We choose $f \in I \setminus (G)$ such that $\mathrm{LT}(f)$ is minimal, which exists because our admissible order is a well order. Let $h \in A$ be an element such that there exist $b, b' \in \mathcal{B}$ with $\mathrm{LT}(f) = b\,\mathrm{LT}(h)b'$. We then have with Proposition 1.43 that $\mathrm{LT}(f) = \mathrm{LT}(bhb')$. By construction, we have $\mathrm{LT}(f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(h)} bhb') \prec \mathrm{LT}(f)$, and by minimality of $\mathrm{LT}(f)$, we must therefore have $f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(h)} bhb' \in (G)$, which then necessarily implies $h \notin G$ (as otherwise we would conclude that $f \in (G)$). What we have just shown is that there is no leading term $\mathrm{LT}(h)$ of an element $h \in G$ that divides $\mathrm{LT}(f)$, which means that $(\mathcal{B} \cdot \mathrm{LT}\{G\} \cdot \mathcal{B}) \setminus \{0\} \subsetneq \mathrm{LT}\{I\}$, concluding our contraposition.

(Compare to [Xiu12, Lem, 3.3.15].) □

Example 1.46. 1. Consider the polynomial ring in one variable $A = k[x]$ with multiplicative basis $[x] = \{x^i \mid i \in \mathbb{N}_0\}$. There is only one possible admissible order on $[x]$, namely $1 \prec x \prec x^2 \prec \cdots$.

For an ideal $I \subseteq A$, there always exists a polynomial $\gcd(I)$, the greatest common divisor of I, such that $I = (\gcd(I))$, because $k[X]$ is Euclidean and therefore a principal ideal domain. The set $G = \{\gcd(I)\}$ then is a reduced Gröbner basis of I. If $I = (f, g)$ is generated by two elements $f, g \in I \setminus \{0\}$, then $G = \{\gcd(f, g)\}$, obtained by performing the euclidean algorithm on f and g, is a reduced Gröbner basis of I.

2. Let $M \in k^{m\times n}$ and $b \in k^m$. Finding solutions to the equation $Ax = b$ corresponds to solving a set of m linear equations in n variables, namely the linear equations defined by $f_i := (\sum_{j=1}^n a_{i,j}x_j) - b_i = 0$ for $i = 1, \ldots, m$. This is the same as asking what the vanishing locus of the ideal $I = (f_1, \ldots, f_m) \subseteq k[x_1, \ldots, x_n]$ is.

   Let $A' \in k^{m\times n}$ and $b' \in k^m$ be the result of the Gaussian algorithm, such that the matrix $(A' \mid b')$ is in row echelon form. If the rank of $(A' \mid b')$ is strictly greater than that of A', then $I = k[x_1, \ldots, x_n]$, and $\{1\}$ is a reduced Gröbner basis of I, and there are no solutions to $Ax = b$. Assume now that there are solutions, meaning that the rank of $(A' \mid b')$ and A' are equal.

   Let $f_i' := (\sum_{j=1}^n a_{i,j}x_j) - b_i'$ for $i = 1, \ldots, m$ be the linear polynomials obtained from the equation $A'x = b'$. Then $\{f_1', \ldots, f_m'\}$ is a Gröbner basis of I for any admissible order on $[x_1, \ldots, x_n]$ such that $x_1 \succ x_2 \succ \cdots \succ x_n$. If $(A' \mid b')$ is in *reduced* row echelon form, then $\{f_1', \ldots, f_m'\} \setminus \{0\}$ is a *reduced* Gröbner basis of I. The same statements can be said about $k\langle X\rangle$.

   For now, we will not explain why we obtain a Gröbner basis in this way, but this example illustrates how we "find" all occurring leading terms in I: If in a row of A', the leftmost nonzero entry is in the j-th column, then $x_j \in \mathrm{LT}(I)$. The Gaussian algorithm is a special case of Buchberger's procedure, and transforming a matrix in row echelon form into a matrix in reduced row echelon form is a special case of tip reduction. Both of these concepts will be discussed later.

   The polynomials $\{f_1', \ldots, f_m'\}$ are in some sense a "nice" set of generators for I. The solutions to $Ax = b$ are an affine linear subspace of k^n, and the way that the f_i' were found, we can then easily find the affine coordinates of this affine linear subspace.

3. Consider $A = k\langle x, y\rangle$ with multiplicative basis $\mathcal{B} = \langle x, y\rangle$ and admissible order $\preceq_{\mathtt{Dp}}$. Define the ideal $I := (f, g)$ for $f = xy + y$ and $g = x + y$. The set $G := \{f, g\}$ is not a Gröbner basis of I, as $h := y^2 - y = g \cdot y - f \in I$, but $\mathrm{LT}(h) = y^2 \notin \mathrm{LT}(G)$. The set $G' := \{g, h\}$ also generates I, and the question is if it is a Gröbner basis of I. It is at the moment not easy to find a convincing argument to prove that something is a Gröbner basis, so we will for now only check some cases for leading terms of polynomials in I.

   Consider $a := p_1 \cdot g \cdot p_1' + p_2 \cdot h \cdot p_2' \in I \setminus \{0\}$ for some $p_1, p_1', p_2, p_2' \in A$. If $\mathrm{LT}(a) = \mathrm{LT}(p_1) \cdot \mathrm{LT}(g) \cdot \mathrm{LT}(p_1')$ or $\mathrm{LT}(a) = \mathrm{LT}(p_2) \cdot \mathrm{LT}(h) \cdot \mathrm{LT}(p_2')$, then clearly $\mathrm{LT}(a) \in \mathrm{LT}(G')$.

   Assume now that this is not the case. This is only possible if the leading terms "cancel each other out", that is we have $\mathrm{LM}(p_1gp_1') = -\mathrm{LM}(p_2hp_2')$. This means $\mathrm{LT}(p_1) \cdot \mathrm{LT}(g) \cdot \mathrm{LT}(p_1') = \mathrm{LT}(p_1gp_1') = \mathrm{LT}(p_2hp_2') = \mathrm{LT}(p_2) \cdot \mathrm{LT}(h) \cdot \mathrm{LT}(p_2')$. Since $\mathrm{LT}(g) = x$ and $\mathrm{LT}(h) = y^2$, we see that these leading terms do not "overlap". We will go more into detail on what this means later, but for now we can just observe how they don't contain any common subword. We therefore must have

- $\mathrm{LT}(p_1') = v \cdot \mathrm{LT}(h) \cdot \mathrm{LT}(p_2')$ and $\mathrm{LT}(p_2) = \mathrm{LT}(p_1) \cdot \mathrm{LT}(g) \cdot v$, or
- $\mathrm{LT}(p_1) = \mathrm{LT}(p_2) \cdot \mathrm{LT}(h) \cdot v$ and $\mathrm{LT}(p_2') = v \cdot \mathrm{LT}(g) \cdot \mathrm{LT}(p_1')$

for some $v \in \langle x, y \rangle$. In any case, we must then have $\mathrm{LT}(g) \mid \mathrm{LT}(a)$ or $\mathrm{LT}(h) \mid \mathrm{LT}(a)$, so $\mathrm{LT}(a) \in \mathrm{LT}(G')$.

Consider now $a = p_1 \cdot h \cdot p_1' + p_2 \cdot h \cdot p_2' \in I \setminus \{0\}$ for some $p_1, p_1', p_2, p_2' \in A$. Again, assume that the leading terms of $p_1 h p_1'$ and $p_2 h p_2'$ in this sum cancel each other out. As above, if $\mathrm{LT}(h) \mid \mathrm{LT}(p)$ for $p \in \{p_1, p_1', p_2, p_2'\}$, then $\mathrm{LT}(a) \in \mathrm{LT}(G')$. But in this case, there are even more possibilities for the leading terms to cancel each other out, so let's cover all of them.

As we cancelled out the leading term, it must be the case that $\mathrm{LT}(a) = \mathrm{LT}(p_1) y \,\mathrm{LT}(p_1')$ or $\mathrm{LT}(a) = \mathrm{LT}(p_2) y \,\mathrm{LT}(p_2')$. Let us assume the former case. If $\mathrm{LT}(p_1)$ is of the form $\mathrm{LT}(p_1) = vx$ for some $v \in \langle x, y \rangle$, then $\mathrm{LT}(g) = x \mid \mathrm{LT}(a)$. If $\mathrm{LT}(p_1)$ is of the form $\mathrm{LT}(p_1) = vy$ for some $v \in \langle x, y \rangle$, then $\mathrm{LT}(h) = y^2 \mid \mathrm{LT}(a)$. If neither is the case, we must have $p_1 = 1$. We can now use the same argument for $\mathrm{LT}(p_1') = xv$ or $\mathrm{LT}(p_1') = yv$ for some $v \in \langle x, y \rangle$. One of these cases must be true, since we cannot have $p_1 = p_1' = 1$, as then we must also have $p_2 = p_2' = 1$ which contradicts the assumption that $a \neq 0$. The case $\mathrm{LT}(a) = \mathrm{LT}(p_2) y \,\mathrm{LT}(p_2')$ is completely analogous, and so in summary, we must have $\mathrm{LT}(a) \in \mathrm{LT}(G)$ in any case.

We can similarly convince ourselves that for $a = p_1 \cdot g \cdot p_1' + p_2 \cdot g \cdot p_2' \in I \setminus \{0\}$ for some $p_1, p_1', p_2, p_2' \in A$, we have $\mathrm{LT}(a) \in \mathrm{LT}(G)$. But what if $a \in I \setminus \{0\}$ is of a different form than the three cases that we covered? We will later see how to ensure that we check everything.

◁

We will see later that indeed every ideal has a unique monic reduced Gröbner basis. The terminology is a bit confusing, since a Gröbner basis is not really a "basis" if we compare it to other common uses of the term. Really, a Gröbner basis should be called a Gröbner generating set, and a reduced Gröbner basis should be called a Gröbner basis. As is usual with terminology in mathematics, we have to stick to the definitions that are already in use.

Theorem 1.47 (Macaulay's basis theorem)**.** *Let $I \subseteq A$ be an ideal. We then have*

$$A = I \oplus \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$$

as vector spaces. ◁

Proof. The vector subspaces I and $\mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$ have trivial intersection, as $f \in \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\}) \setminus \{0\}$ implies $\mathrm{LT}(f) \notin \mathrm{LT}\{I\}$, which in turn implies $f \notin I$. Now let us show that $A = I + \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$.

Assume towards a contradiction that $A \supsetneq I + \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$. Choose a nonzero $f \in A \setminus (I + \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\}))$ with minimal $\mathrm{LT}(f)$, which is possible because $\preceq$ is a well order.

Assume first that $\mathrm{LT}(f) \in \mathcal{B} \setminus \mathrm{LT}\{I\}$. Consider $g := f - \mathrm{LM}(f)$, for which we have $\mathrm{LT}(g) \prec \mathrm{LT}(f)$ by construction. By minimality of $\mathrm{LT}(f)$, we must therefore have $g \in I + \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$, say of the form $g = y + r$ with $y \in I$ and $r \in \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$. But then $r + \mathrm{LM}(f) \in \mathrm{span}_k(\mathcal{B} \setminus I)$, which leads to a contradiction because $f = g + \mathrm{LM}(f) = y + r + \mathrm{LM}(f) \in I + \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$.

Assume now that $\mathrm{LT}(f) \in \mathrm{LT}\{I\}$, which means we can choose $h \in I$ such that $\mathrm{LM}(h) = \mathrm{LM}(f)$. For $g := f - h$, we then have $\mathrm{LT}(g) \prec \mathrm{LT}(f)$ by construction. By minimality of $\mathrm{LT}(f)$, we must then have $g \in I + \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$, say $g = y + r$ with $y \in I$ and $r \in \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$. But with $h + y \in I$, we then have $f = h + g = (h + y) + r \in I + \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$, which is a contradiction.

(Compare to [Gre99, Theorem 2.1] and [Xiu12, Corollary 3.1.16].) □

Remark 1.48. The multiplicative structure on A is irrelevant for Theorem 1.47, the proof works for any vector space V with basis $\mathcal{B}$ and a well order $\preceq$ on $\mathcal{B}$, and $I \subseteq V$ is any linear subspace. ◁

Definition 1.49 (normal form, remainder)**.** In the situation of Theorem 1.47, for an element $y \in A$, we can uniquely write

$$y = i_y + \mathrm{N}(y; I)$$

with $i_y \in I$ and $\mathrm{N}(y; I) \in \mathrm{span}_k(\mathcal{B} \setminus \mathrm{LT}\{I\})$, and we call $\mathrm{N}(y; I)$ the **normal form** of y for I, or the **normal remainder** of the division of y by I. We also say that y **reduces** to r with respect to I. ◁

Lemma 1.50. Let $I \subseteq A$ be a monomial ideal. Then I has a unique minimal monomial generating set $M \subseteq \mathcal{B}$ of I. ◁

Proof. Define $M := \{f \in I \cap \mathcal{B} \mid g \in I \cap \mathcal{B},\ g \mid f \implies g = f\}$. Choose any monomial $f \in I \cap \mathcal{B}$, and consider the set $D(f) := \{b' \in I \cap \mathcal{B} \mid b' \mid f\}$. We have $f \mid f$ and therefore $f \in D(f)$, so $D(f)$ is nonempty. There exists a minimal such element $d(f) \in D(f)$ with respect to our order $\preceq$, as it is a well order. But since our well order is also an admissible order, for any monomial $b' \in I \cap \mathcal{B}$ with $b' \mid s$, we must have $b' \preceq d(f)$ by (O2), and by minimality of f then $b' = d(f)$, so $d(f) \in M$. This also shows that M is nonempty.

Now we show that M generates I. Notice that since I is a monomial ideal, $I \cap \mathcal{B}$ generates I, in fact I is just the k-span of $I \cap \mathcal{B}$. It therefore suffices to show that for every $h \in I \cap \mathcal{B}$, there is an $m \in M$ that divides h. But this is already case for $m = d(h) \in D(h)$ by construction.

We now show that M is minimal. Let M' be another monomial generating set of I. Then for $m \in M$ there must exist an $m' \in M'$ such that $m' \mid m$. But by definition of M, we must have $m' = m$, so $M \subseteq M'$. This shows that M is the unique minimal monomial generating set of I, concluding our proof.

(Compare to [Gre99, Prop. 2.5].) □

Remark 1.51. Lemma 1.50 is really a statement about semirings, as for a monomial ideal I generated by a set $T \subseteq \mathcal{B}$, the ideal I is just the span of the subsemiring in $\mathcal{B}_0$ generated by T, which is $I \cap \mathcal{B}$, as noted in the proof. ◁

Theorem 1.52. *Let A be a k-algebra with multiplicative basis $\mathcal{B}$ with an admissible order, and let I be an ideal in A. Let $\mathcal{T}$ be the minimal monic generating set of* $\mathrm{LT}(I)$ *as in Lemma 1.50. Then*

$$G = \{t - \mathrm{N}(t; I) \mid t \in \mathcal{T}\}$$

is the unique monic reduced Gröbner basis of I. ◁

Proof. Let us check the conditions in Definition 1.44.

For any $t \in \mathcal{T}$, we have $t - \mathrm{N}(t; I) \in I$, so we have $\mathrm{LT}(t - \mathrm{N}(t; I)) \in \mathrm{LT}\{I\}$, and with $\mathrm{N}(t; N) \in \mathrm{span}(\mathcal{B} \setminus \mathrm{LT}\{I\})$, we get $\mathrm{LT}(t - \mathrm{N}(t; I)) = t$. We have now shown $\mathrm{LT}\{G\} = \mathcal{T}$, and $\mathrm{LT}\{G\}$ is a minimal generating set of $\mathrm{LT}(I)$ via construction of $\mathcal{T}$, and we have also shown that G is monic.

Let $g \in G$, so $g = t - \mathrm{N}(t; I)$ for some $t \in \mathcal{T}$. We can then compute

$$\begin{aligned} g - \mathrm{LM}(g) &= g - \mathrm{LT}(g) \\ &= t - \mathrm{N}(t; I) - \mathrm{LT}(t - \mathrm{N}(t; I)) \\ &= t - \mathrm{N}(t; I) - t \\ &= -\mathrm{N}(t; I) \in \mathrm{span}(\mathcal{B} \setminus \mathrm{LT}\{I\}) \,. \end{aligned}$$

It remains to show $(G) = I$. Assume towards a contradiction that there exists $f \in I$ such that $f \notin (G)$, and choose such an f with minimal leading term $\mathrm{LT}(f)$. As $(\mathcal{T}) = \mathrm{LT}(I)$, there exists $t \in \mathcal{T}$ such that $t \mid \mathrm{LT}(f)$, say $\mathrm{LT}(f) = btb'$ for $b, b' \in \mathcal{B}$. Define $h := b \cdot \mathrm{LC}(f)(t - \mathrm{N}(t; I)) \cdot b' \in (G) \subseteq I$. By the above calculations in this proof, we again have $\mathrm{LT}(t - \mathrm{N}(t; I)) = t$, and therefore also $\mathrm{LT}(h) = btb'$, and we have $f - h \in I$. If $f = \mathrm{LC}(f)(t - \mathrm{N}(t; I))$, we have a contradiction as $h \in (G)$, but we assumed $f \notin (G)$. If $f \neq h$, then by construction $\mathrm{LT}(f - h) \prec \mathrm{LT}(f)$. By minimality of $\mathrm{LT}(f)$ we must then have $f - h \in (G)$, but then $f = f - h + h \in (G)$, which is a contradiction to our assumption $f \notin (G)$.

We have now shown that G is a monic reduced Gröbner basis, let us now show that it is unique. Let H and H' be monic reduced Gröbner bases of I, and let $h \in H$. We must have $\mathrm{LT}\{H\} = \mathcal{T} = \mathrm{LT}(H')$ by (1) in Definition 1.44. Therefore, for $h \in H$, there is $h' \in H'$ such that $\mathrm{LT}(h) = \mathrm{LT}(h')$, and since they are both monic, we also have $\mathrm{LM}(h) = \mathrm{LM}(h')$. Together with (2) in Definition 1.44, we then get

$$\begin{aligned} h - h' &= h - \mathrm{LM}(h) + \mathrm{LM}(h) - h' \\ &= h - \mathrm{LM}(h) - (h - \mathrm{LM}(h') \in \mathrm{span}(\mathcal{B} \setminus \mathrm{LT}\{I\}) \,. \end{aligned}$$

But since $h - h' \in I$, and $I \cap \mathrm{span}(\mathcal{B} \setminus \mathrm{LT}\{I\}) = \{0\}$, we must have $h = h'$. □

2. Algorithms For Gröbner Bases

So far, it is not really clear what Gröbner bases are there for. Algebras with a multiplicative basis are very common, but the introduction of an admissible order is not really something that is seen outside of the theory of Gröbner bases. For the nature of the algebra, the admissible order we choose itself as a structure is not really important, but we will rather see that this is a necessary tool to generalize concepts we know from other areas. In Definition 1.49 we defined a notion of a **remainder**, somehow implying that there is some kind of division taking place. This is what will be discussed in this chapter.

Let us think about the intuition of "dividing" in conjunction with orders. In euclidean domains, we have something similar to an order via the euclidean function. For the example of the polynomial ring in one variable $k[x]$, the euclidean function is just the degree. This function restricted to the multiplicative basis $\mathcal{B} = \{1, x^1, x^2, \ldots\}$ is the canonical weight function (weight vector (1)), but in fact it doesn't matter what weight function we choose, any weight function and any prior total order as in Definition 1.32 will lead to the same admissible order, and even without this construction we can easily come to the realisation $\mathcal{B}$ has a unique admissible order, as was described in Example 1.46.1. Now, with this admissible order, decomposing as in Definition 1.49 is the same as division with remainder as defined in euclidean domains. So we see that the concepts talked about in the previous chapter arise naturally for the special case of $k[x]$. In this chapter, our goal is to now also generalize the algorithmic aspect of the division and the computation of a greatest common divisor.

In this chapter, if not stated otherwise, A is a k-algebra with multiplicative basis $\mathcal{B}$ and admissible order $\preceq$.

2.1. Division with remainder

There is a subtlety when talking about ideals and divisibility. In commutative rings, "$a \mid b$" is equivalent to $b \in (a)$, but for noncommutative rings, this is not always the case. For instance, consider $R = k\langle x, y\rangle$, where we have $xy + yx \in (x)$, but $x \nmid xy + yx$. Eventhough we use the same term "division" as in the commutative setting, we don't want to have "$a \mid b$", but instead "$a \in (b)$" when we perform a division of b by a with remainder 0 in the noncommutative setting. But what is a division with remainder then?

Let $F \subseteq A$ be a subset and let $y \in A$. We want to "divide" y by the polynomials in F with remainder. A sensible definition for a division with remainder is the following. For every $f \in F$, we choose nonnegative integers $k_f \in \mathbb{N}_0$ and elements $u_{f,j}, v_{f,j} \in A$ for $f \in F$ and $i \in [k_x]$, and an $r \in A$ such that

- $y = \sum_{f \in F}(\sum_{j \in [k_f]} u_{f,j} f v_{f,j}) + r$,
- $\mathrm{LC}(u_{f,i} f v_{f,i}) \preceq \mathrm{LC}(y)$ for all $f \in F$ and $i \in [k_f]$, and
- for all $b \in \mathrm{supp}(r)$, $\mathrm{LC}(f) \nmid b$ for all $f \in F$.

It is not clear that such a presentation always exists, but we will see that this is the case. If we remember our procedure of the division in the polynomial ring in one variable $k[x]$, we want to decompose it even further by choosing our $u_{f,j}$ and $v_{f,j}$ to be in $\mathcal{B}$ up to a scalar multiple, which is also possible here as $\mathcal{B}$ is a k-basis. So what we really want is the following.

Definition 2.1 (division, remainder)**.** Let A be a k-algebra with multiplicative basis $\mathcal{B}$ and admissible order $\preceq$. Let $F \subseteq A$ be a subset of A and let $y \in A$. Assume that we can find for every $f \in F$ nonnegative integers $k_f \in \mathbb{N}_0$, elements $w_{f,j}, w'_{f,j} \in \mathcal{B}$ and $c_{f,j} \in k^\times$ for $f \in F$ and $i \in [k_x]$, and an $r \in A$ such that

1. $y = \sum_{f \in F}(\sum_{j \in [k_f]} c_{f,j} w_{f,j} f w'_{f,j}) + r$,
2. $\mathrm{LT}(w_{f,j} f w'_{f,j}) \preceq \mathrm{LT}(y)$ for all $f \in F$ and $j \in [k_f]$, and
3. for all $b \in \mathrm{supp}(r)$ we have $b \notin \mathrm{LT}(F)$.

We then call such a representation a **division** of y by F, and r is the **remainder**. We also say that we can **reduce** y to r with respect to F.
(Compare to [Xiu12, p. 34].) ◁

Remark 2.2.
1. It follows from (2) in Definition 2.1 that we have $\mathrm{LT}(r) \leq \mathrm{LT}(y)$.
2. We must have either $\mathrm{LT}(y) = \mathrm{LT}(r)$ or $\mathrm{LT}(y) = w_{f,j} f w'_{f,j}$ for some $f \in F$ by the previous remark and by (2) in Definition 2.1.
3. In (3) of Definition 2.1, as $b \in \mathcal{B}$, this is equivalent to requiring $\mathrm{LT}(f) \nmid b$ for all $f \in F$.

◁

Reducing y to r with respect to F, and calling r the remainder of the division by F as in definition 2.1 is not necessarily the same as the normal form defined of y with respect to (F) as in definition 1.49. We will soon see that there is a connection between these two definitions.

The division in definition 2.1 suggests that these $w_{f,j}, w'_{f,j}, c_{f,j}$ and r do exist, and indeed, we can do this algorithmically. The algorithm works as follows (taken from [Xiu12, Theorem 3.2.1]):

1. We initialise $k_f := 0$ for $f \in F$ and $r := 0$, $z := y$.
2. Find the first element of $f \in F$ (assume that F is implemented as a list) such that $\mathrm{LT}(f)$ divides $\mathrm{LT}(z)$, id est there exist $w, w' \in \mathcal{B}$ such that $\mathrm{LT}(z) = w\,\mathrm{LT}(f)w'$. If it exists, increase k_f by one, set $c_{f,k_f} := \mathrm{LC}(v)/\mathrm{LC}(f)$, $w_{f,k_f} := w$, $w_{f,k_f} := w'$ and replace z by $z - \mathrm{LC}(z)/\mathrm{LC}(f)wfw'$.
3. Repeat step 2 until no such $f \in F$ exists anymore.
4. If $z \neq 0$, replace r by $r + \mathrm{LT}(z)$ and z by $z - \mathrm{LT}(z)$, and go back to step 2. If $z = 0$, we are done.

Let us write this down in pseudo-code (compare with [Gre99, p. 38] [it very much looks like the algorithm in this source is faulty/wrong/has errors]).

Proposition 2.3. *The division algorithm (algorithm 1) terminates and yields a division as in definition 2.1.*

(Compare to [Gre99, p. 2.3.2] and [Xiu12, Theorem 3.2.1]) ◁

Algorithm 1 Division Algorithm

Input: finite set $F \subseteq R$, $y \in A$

Output: $k_f \in \mathbb{N}_0$ for $f \in F$; $w_{f,j}, w'_{f,j} \in \mathcal{B}$ and $c_{f,j} \in k$ for $f \in F$, $j \in k_f$; $r \in A$; such that $y = \sum_{f\in F}(\sum_{j\in[k_f]} c_{f,j}w_{f,j}fw'_{f,j}) + r$, $\mathrm{LT}(w_{f,j}fw'_{f,j}) \preceq \mathrm{LT}(y)$ for all $f \in F$ and $j \in [k_f]$, and $b \notin \mathrm{LT}\{F\}$ for all $b \in \mathrm{supp}(r)$.

```
1:  k_f ← 0 for all f ∈ F
2:  r ← 0
3:  z ← y
4:  while z ≠ 0 do
5:      if ∃f ∈ F, ∃w, w' ∈ B: LT(z) = w LT(f)w' then
6:          k_f ← k_f + 1
7:          c_{f,k_f} ← LC(z)/LC(f)
8:          w_{f,k_f} ← w
9:          w'_{f,k_f} ← w'
10:         z ← z − (LC(z)/LC(f))wfw'
11:     else
12:         r ← r + LM(z)
13:         z ← z − LM(z)
```

Proof (sketch). In every iteration of the "while" loop, the leading coefficient of z gets strictly decreased, and our admissible order is a well order, z must reach 0 eventually, so the algorithm does terminate.

By the same argument, we also have that $\mathrm{LT}(y) \preceq \mathrm{LT}(z) = w_{f,k_f}\,\mathrm{LT}(f)w'_{f,k_f}$ after every iteration where the if case is true. Note that after this iteration, k_f is not the final value of k_f, rather this value goes through every value from 0 to the final value of k_f.

Therefore we see that at the end of the algorithm, we have $\mathrm{LT}(w_{f,j} f w'_{f,j}) \preceq \mathrm{LT}(y)$ for all $f \in F$ and all $j \in [k_f]$.

After every iteration of the "while" loop, by construction we clearly have $y = z + \sum_{f\in F}(\sum_{j\in[k_f]} c_{f,j} w_{f,j} f w'_{f,j}) + r$, and since $z = 0$ after the last iteration, we have $y = \sum_{f\in F}(\sum_{j\in[k_f]} c_{f,j} w_{f,j} f w'_{f,j}) + r$.

Lastly since the else case only is true if for every $f \in F$ the leading term $\mathrm{LT}(f)$ doesn't divide $\mathrm{LT}(z)$, we have $\mathrm{LT}(z) \nmid \mathrm{LT}(f)$ for all $f \in F$, which is equivalent to $\mathrm{LT}(z) \notin \mathrm{LT}\{F\}$. Since r is just a sum of all such $\mathrm{LM}(z)$, we have $b \notin \mathrm{LT}\{F\}$ for all $b \in \mathrm{supp}(r)$. □

The algorithm, as is, is not deterministic. In our if clause, it is not clear which $f \in F$ and which $w, w' \in \mathcal{B}$ we should choose.

Algorithmically, a set F is usually implemented as some kind of a list $\mathcal{F}$, so checking the if condition is done in order of the enumeration of the set F. If we live in an ordered field, for example $k = \mathbb{R}$, it is also possible to find a total order on A, and we could check the elements in F in descending or ascending order with respect to that total order.

After this, we then have to choose for a fixed $f \in F$ a strategy for which $w, w' \in \mathcal{B}$ that fulfill the if condition. We can easily construct a well order on $\mathcal{B} \times \mathcal{B}$, for example the lexicographic order as in Definition 1.21, which gives us a strategy to check if $w, w' \in \mathcal{B}$ fulfill the if condition. Here, it is in general important that we choose a well order, because our strategy would be to find the minimal w, w' such that the if condition is fulfilled, and the existence of such a minimal element is given by being well-ordered.

Abstractly, this is gives us a well-defined deterministic algorithm. But in practice, we of course run into problems if this well-ordered set is not isomorphic to $\mathbb{N}_0$, because we then can't check all possibilities in ascending order. This for example would be the case if we define our well order on $\mathcal{B} \times \mathcal{B} = \mathcal{B}^2$ via the lexicographic order as in Definition 1.21.

But more specifically in practice, we work with quiver algebras or polynomial rings, and there the set of possible $w, w' \in \mathcal{B}$ in each step for a fixed $f \in F$ is always finite, which can be easily verified by degree arguments. Therefore, in this case, taking any total order on $\mathcal{B} \times \mathcal{B}$ even works algorithmically.

Definition 2.4. Assume we implement F as list, so $\mathcal{F} = (f_1, \dots, f_{|F|})$, and if we have a deterministic method for choosing w and w' such that $\mathrm{LT}(z) = w\,\mathrm{LT}(f)w'$, then Proposition 2.3 is truly deterministic by having a fixed order for the checks to be executed.

We then have a well-defined map that maps an element y and an ordered list $\mathcal{F}$ to the remainder r of the division of y by $\mathcal{F}$ and write $\mathrm{N}(y; \mathcal{F})$, which might be a slight abuse of notation, since the result can vary according to how we choose $\mathcal{F}$ from F, so $\mathrm{N}(y, F)$ is not well-defined in general and we therefore cannot in general write $\mathrm{N}(y; \mathcal{F}) = \mathrm{N}(y; (F))$. ◁

From now on, $\mathrm{N}(\bullet; \bullet)$ will refer to some fixed choice of a function as described in Definition 2.4.

If we perform a division of an element y by a set F and we get remainder 0, then it is clear that $y \in (F)$. But do we get remainder 0 if $y \in (F)$? The answer is no, not in general.

Example 2.5. Consider $A = k\langle x, y\rangle$, $h = xy^2$, and the set $G = \{g_1, g_2\}$ for $g_1 = x^2 - xy$ and $g_2 = xyx$. We have $h = g_1(x - y) - xg_1 + g_2$, so $h \in (G)$. Let us now perform a division of h by G like in proposition 2.3.

- The first time we go through our "while" loop, the if-case won't be fulfilled for either g_1 or g_2.
- We set $r = xy^2$ and $z = 0$.
- We are done as $z = 0$.

As we see, eventhough $h \in (G)$, we have a division of h by G with a nonzero remainder. We can also check this in SINGULAR.

```
> LIB "freegb.lib";
> ring r = 0,(x,y),dp;
> def A = freeAlgebra(r,20);
> setring A;
> ideal G = x*x - x*y, x*y*x;
> reduce(x*y*y,G);

// ** G is no standard basis
x*y*y
```

SINGULAR even helpfully informs us `G is no standard basis`, hinting the exact problem we constructed: xy^2 is in the ideal generated by G, but the normal remainder with respect to G in the implementation of SINGULAR is not 0. ◁

2.2. An example for different reduction strategies

In this example, we will construct examples where we see how different strategies lead to different outcomes, and how SINGULAR deals with this.

Consider $k\langle x, y\rangle$ and the elements $f = xy + x$, $g = x - y$ and $h = xyx - x$. We want to reduce h with respect to f and g. Depending on the order of f and g, we should get different results in the division algorithm. Let us go through the algorithm with the enumeration $\mathcal{F} = (f, g)$, and the strategy of choosing the smallest w, in other words the smallest $(w, w') \in \mathcal{B} \times \mathcal{B}$ with respect to the left lexicographic order on $\mathcal{B} \times \mathcal{B}$.

1. $r = 0$, $z = h = xyx - x$.
2. $\mathrm{LT}(f) \mid \mathrm{LT}(z)$, and we set
   - $w_{f,1} = 1$, $w'_{f,1} = x$, $c_{f,1} = 1$, and
   - $z = xyx + x - fx = -x^2 + x$.
3. $\mathrm{LT}(f) \nmid \mathrm{LT}(z)$, but we have $\mathrm{LT}(g) \mid \mathrm{LT}(z)$, so we set
   - $w_{g,1} = 1$, $w'_{g,1} = x$, $c_{g,1} = -1$, and

- $z = -x^2 + x - (-gx) = -yx - x$.

4. $\mathrm{LT}(f) \nmid \mathrm{LT}(z)$, but we have $\mathrm{LT}(g) \mid \mathrm{LT}(z)$, so we set
   - $w_{g,2} = y$, $w'_{g,2} = 1$, $c_{g,2} = -1$, and
   - $z = -yx + x - (-yg) = -y^2 - x$.
5. $\mathrm{LT}(f), \mathrm{LT}(g) \nmid \mathrm{LT}(z)$, so we set
   - $z = -x$,
   - and $r = -y^2$.
6. $\mathrm{LT}(f) \nmid \mathrm{LT}(z)$, but we have $\mathrm{LT}(g) \mid \mathrm{LT}(z)$, so we set
   - $w_{g,2} = 1$, $w'_{g,2} = 1$, $c_{g,2} = 1$, and
   - $z = -x - (-g) = -y$.
7. $\mathrm{LT}(f), \mathrm{LT}(g) \nmid \mathrm{LT}(z)$, so we set
   - $z = 0$ and
   - $r = -y^2 - x$,

   arriving at our final result.

Let's see what happens when we input this into SINGULAR.

```
> LIB "freegb.lib";
> ring r = 0,(x,y),Dp;
> def A = freeAlgebra(r,20);
> setring A;
> ideal F =  x*y - x, x-y;
> reduce(x*y*x - x, F)

// ** F is no standard basis
y*y*y-y
```

So apparently SINGULAR does not use this strategy. Let us try to use the strategy where we take the smallest element with respect to the reverse lexicographic order.

1. Same as above.
2. Same as above.
3. $\mathrm{LT}(f) \nmid \mathrm{LT}(z)$, but we have $\mathrm{LT}(g) \mid \mathrm{LT}(z)$, so we set
   - $w_{g,1} = x$, $w'_{g,1} = 1$, $c_{g,1} = -1$, and
   - $z = -x^2 + x - (-xg) = -xy - x$.
4. $LT(f) \mid \mathrm{LT}(z)$, so we set

- $w_{f,2} = 1$, $w'_{f,2} = 1$, $c_{f,2} = -1$, and
- $z = -xy - x - (-f) = 0$,

arriving at our final result.

So in this case, we actually get remainder 0, so indeed we do have $h \in (f, g)$, in particular still not the strategy SINGULAR uses.

Let us do one more try: We reverse the order of f and g, so we first start checking g and then f, and for w and w' we choose the smallest element with respect to the lexicographic order.

1. $r = 0$, $z = h = xyx - x$
2. $\mathrm{LT}(g) \mid \mathrm{LT}(z)$, so we set
   - $w_{g,1} = 1$, $w'_{g,1} = yx$, $c_{g,1} = 1$, and
   - $z = xyx - x - gyx = y^2x - x$.
3. $\mathrm{LT}(g) \mid \mathrm{LT}(z)$, so we set
   - $w_{g,2} = y^2$, $w'_{g,2} = 1$, $c_{g,2} = 1$, and
   - $z = y^2x - x - y^2g = y^3 - x$.
4. $\mathrm{LT}(g), \mathrm{LT}(f) \nmid \mathrm{LT}(z)$, so we set
   - $z = -x$
   - and $r = y^3$.
5. $\mathrm{LT}(g) \mid \mathrm{LT}(z)$, so we set
   - $w_{g,3} = 1$, $w'_{g,3} = 1$, $c_{g,3} = -1$, and
   - $z = -x - (-g) = -y$.
6. $\mathrm{LT}(g), \mathrm{LT}(f) \nmid \mathrm{LT}(z)$, so we set
   - $z = 0$
   - and $r = y^3 - y$,

   arriving at our final result.

This is the same result as the one SINGULAR produced above. We can also see that SINGULAR produces the same result if we change the order of the elements in the ideal, which is also interesting.

```
> ideal F =  x-y, x*y - x;
> reduce(x*y*x - x, F)

// ** F is no standard basis
y*y*y-y
```

We can construct a scenario in SINGULAR where the order matters. Consider the elements $f = xy + x$, $g = xy + y$ and $h = xyx + x$. We want to reduce h with respect to f and g. Depending on the order of f and g, we will get different results in the division algorithm. We can see this in SINGULAR.

```
> LIB "freegb.lib";
> ring r = 0,(x,y),Dp;
> def R = freeAlgebra(r,20);
> setring R;
> ideal F =  x*y + x, x*y + y;
> reduce(x*y*x + x, F);

// ** F is no standard basis
-y*x+x

> ideal F =  x*y + y, x*y + x;  // Change the order of the elements
> reduce(x*y*x + x, F);

// ** F is no standard basis
-x*x+x
```

With all that we tried above, we see that the strategy of `reduce` in SINGULAR probably does not correspond to choosing a fixed order for `F`. SINGULAR probably reorders the elements of `F`, probably by their leading term. If the elements in `F` all have the same leading term, then it seems that SINGULAR does not reorder them, as seen in this example.

2.3. Gröbner representations

So far, what we have defined a "division" does not feel quite right, because ideally we want to have a division by a set that gives us remainder 0 if and only if an element be expressed by a two-sided A-linear combination of that set.

As mentioned before, if we can reduce an element $y \in A$ to 0 with respect to F, then this means that $y \in (F)$. We actually have something stronger by our requirements in definition 2.1 of the division. This motivates the following definition.

Definition 2.6 (Gröbner representation)**.** For $y \in A$, we call a representation

$$y = \sum_i c_i w_i g_i w_i'$$

with $c_i \in k^\times$, $g_i \in F$, and $w_i, w_i' \in \mathcal{B}$ a **Gröbner representation** of y in terms of F if $\mathrm{LT}(w_i g_i w_i') \preceq \mathrm{LT}(y)$ for all i. ◁

Remark 2.7. If it wasn't clear by the narrative, y has a Gröbner representation in terms of F if and only if we can reduce y to 0 with respect to F. ◁

What we want still is a well-defined reduction for any element in A, meaning a map that gives us some specific remainder of a division. So far, Definition 2.1 doesn't give us uniqueness of the remainder, and indeed, as we have seen, we don't have uniqueness in general. This is where Gröbner bases come into play.

Proposition 2.8. *In the context of Definition 2.1, if F is a Gröbner basis for $I = (F)$, then the remainder r of the division of an element $y \in A$ by F is unique. This also means that in the context of Proposition 2.3, we have $\mathrm{N}(y;\mathcal{F}) = \mathrm{N}(y;\mathcal{F}')$ for any enumerations $\mathcal{F}, \mathcal{F}'$ of F, and we have $r = \mathrm{N}(y;I)$ (Definition 1.49).* ◁

Proof. Let $y = a + r$ with $a = \sum_{f\in F}(\sum_{j\in[k_f]} u_{f,j} f v_{f,j})$ be a division as described in Definition 2.1. Since we have for all $b \in \mathrm{supp}(r)$ that $\mathrm{LC}(f) \nmid b$ for all $f \in F$, we have $r \in \mathrm{span}\{\mathcal{B} \setminus \mathrm{LT}(I)\}$, precisely because G is a Gröbner basis of I. Since $a \in I$, we must have $a = i_y$ and $r = \mathrm{N}(y;I)$ as in Theorem 1.47. □

We have now shown that if G is a Gröbner basis for $I = (G)$, in light of Proposition 2.8, we can write $\mathrm{N}(y;G) = \mathrm{N}(y;I)$. Now, finally, we can justify our notion of a division.

Proposition 2.9. *The set G is a Gröbner basis for an ideal I if and only if every $f \in (G) \setminus \{0\}$ has a Gröbner representation in terms of G.* ◁

Proof. Let $G \subseteq I$ be a Gröbner basis of I, and let $f \in I$.

Let $v_0 := f$, and recursively define $v_{n+1} = 0$ if $v_n = 0$, and otherwise define $v_{n+1} := v_n - c_{n+1} w_{n+1} g_{n+1} w'_{n+1}$, where $\mathrm{LT}(v_n) = w_{n+1}\,\mathrm{LT}(g_{n+1})w'_{n+1}$ for some $g_{n+1} \in G$, $w_{n+1}, w'_{n+1} \in \mathcal{B}$ and $c_{n+1} := \mathrm{LC}(v_n)/\,\mathrm{LC}(g_{n+1})$. This is always possible, because G is a Gröbner basis. We have $\mathrm{LC}(v_n) \succ \mathrm{LC}(v_{n+1})$ for every $n \in \mathbb{N}_0$ such that $v_{n+1} \neq 0$, and since our admissible order is a well order, $v_n = 0$ after some large enough index certain index. Let $m \in \mathbb{N}_0$ be the first index such that $v_n = 0$ for all $n \geq m$. Then by construction we have $f = \sum_{i\in[m]} c_i w_i g_i w'_i$ and $\mathrm{LT}(f) \preceq \mathrm{LT}(w_i g_i w'_i)$ for all $i \in [m]$, so f has a Gröbner representation.

Assume that every nonzero $f \in I$ has a Gröbner representation. Then clearly $(G) = I$. If $f = \sum_i c_i w_i g_i w'_i$ is a Gröbner representation of $f \in I \setminus \{0\}$, then $\mathrm{LT}(f) = w_j\,\mathrm{LT}(g_j)w'_j$ for some j because $\mathrm{LT}(f) \succeq w_i\,\mathrm{LT}(g_i)w'_i$ for all i, and therefore $\mathrm{LT}(f) \in \mathrm{LT}(G)$. Therefore $\mathrm{LT}(I) = \mathrm{LT}(G)$, making G a Gröbner basis of I.

(Compare to [Xiu12, Proposition 3.3.6]) □

Corollary 2.10. *With Proposition 2.9 and Proposition 2.8, G is a Gröbner basis of I if and only if $\mathrm{N}(f;\mathcal{G}) = 0$ for some enumeration $\mathcal{G}$ of G, or equivalently for any enumeration $\mathcal{G}$ of G.* ◁

This is exactly what Gröbner bases do. We noted before that if we have generators of an ideal, our notion of a division doesn't give us a way to check if an element can be expressed as an A-linear combination of these generators, as seen in Example 2.5. If we pick special generators though, special here meaning we have a Gröbner basis, our division does give us exactly that. This is one of the key intuitions behind Gröbner bases. They are in some sense the best representatives of an ideal, the generators which give us a good notion of a division.

Corollary 2.11 (ideal membership)**.** *If G is a Gröbner basis for $I = (G)$, then for all $y \in A$ we have*

$$y \in I \iff \mathrm{N}(y; G) = 0 \, .$$

◁

Let us sum up what we have learned so far.

- Admissible orders give us a notion of a division with remainder, which is algorithmically implementable, but this is in general not unique.
- An element having remainder 0 for a division by a set G implies that it is contained in the ideal (G).
- If G is a Gröbner basis for (G), then the previous statement is an if and only if statement.
- A Gröbner basis gives us a well-defined map for the remainder of the division by G, and a way to algorithmically check if an element belongs to an ideal.

Corollary 2.11 is also the beginning of our quest to Buchberger's procedure. If we have generators of an ideal and can find elements that are contained in the ideal but are not reduced to 0 after division by these generators, we can add that element to the set of generators and check again. We want to do this until every element in the ideal has remainder 0. But which elements in the ideal do we check? This is where we develop the theory of **obstructions** and **S-polynomials**.

2.4. Obstructions and S-polynomials

In this section, we discuss the theory of obstructions and S-polynomials to compute Gröbner bases as in [Xiu12, Chapter 3.4, Chapter 4.1], and we try to generalize this as much as possible to k-algebras A with multiplicative basis $\mathcal{B}$ and admissible order $\preceq$.

Definition 2.12 (syzygy)**.** We define the A bimodule

$$F_G := (A \otimes A)^G = \{f \colon G \to A \otimes A\}$$

with basis elements ϵ_g for $g \in G$ (such that $\epsilon_g(h) = \delta_{g,h} \otimes \delta_{g,h}$). We define two evaluation morphisms defined by

$$\begin{aligned} \lambda \colon F_G &\to (G) & \epsilon_g &\mapsto g \\ \Lambda \colon F_G &\to \mathrm{LT}(G) & \epsilon_g &\mapsto \mathrm{LM}(g) \, . \end{aligned}$$

The (two-sided) **syzygy** of G and $\mathrm{LM}(G)$, respectively, are

$$\mathrm{Syz}(G) := \ker \lambda \qquad \mathrm{Syz}(\mathrm{LM}(G)) := \ker \Lambda \, .$$

◁

Definition 2.13 (degree, leading form)**.** Let $G \subseteq A$ be a subset. Let $m \in F_G$. If we write $m = \sum_{g\in G} \mu_g u_g \epsilon_g w_g$ with We define the **degree** of m as

$$\deg(m) := \max_{\preceq}(\operatorname{supp}(\Lambda(m))) \in \mathcal{B}$$

if $\Lambda(m) \neq 0$, and $\deg(m) = 0$ otherwise.

With this degree function, we can decompose $F_G = \bigoplus_{b\in\mathcal{B}_0}(F_G)_b$ into its **homogeneous components**, where $(F_G)_b = \operatorname{span}_k\{u\epsilon_g w \mid g \in G, u, w \in \mathcal{B}, u\operatorname{LT}(g)w = b\}$. The homogeneous component of degree $\deg m$, the **leading form** of m, is denoted by $\operatorname{LF}(m)$. ◁

Definition 2.14 (obstruction)**.** Let A be a k-algebra with multiplicative basis $\mathcal{B}$ and an admissible order, and let $G \subseteq A$ be a subset. We define for $g, h \in G$, $v, v', w, w' \in A$ elements

$$o_{g,h}(v, v'; w, w') := \frac{1}{\operatorname{LC}(g)} v\epsilon_g v' - \frac{1}{\operatorname{LC}(h)} w\epsilon_h w' \in F_G\ .$$

If $v, v', w, w' \in \mathcal{B}_0$ and $o_{g,h}(v, v'; w, w') \in \operatorname{Syz}(\operatorname{LT}(G))$, which means that $\Lambda(o_{g,h}(v, v'; w, w')) = 0$ and therefore $v\operatorname{LT}(g)v' = w\operatorname{LT}(h)w'$, we call $o_{g,h}(v, v'; w, w')$ an **obstruction** of g and h. If $g = h$, we call it a **self obstruction**.

The set of all such obstructions of g and h shall be denoted by $o(g, h)$. The union of all these are called obstructions of G and shall be denoted by $o(G)$. ◁

Lemma 2.15. The set $o(G)$ generates $\operatorname{Syz}(\operatorname{LM}(G))$ as an ideal, in fact even as a vector space. ◁

Proof. Let $m = \sum_{g\in G}\sum_i c_{g,i} w_{g,i}\epsilon_g w'_{g,i} \in \operatorname{Syz}(\operatorname{LM}(G))$ with $c_{g,i} \in k^\times$ and $w_{g,i}, w'_{g,i}$ be a homogeneous syzygy of $\operatorname{LM}(G)$. If the degree is 0, we immediately have $w_{g,i}\epsilon_g w'_{g,i} = w_{g,i}\epsilon_g w'_{g,i} - 0 \cdot \epsilon_g \cdot 0 \in o(g, g)$ for all i and $g \in G$.

Now assume the degree is nonzero and assume without loss of generality that all terms $w_{g,i}\epsilon w'_{g,i}$ are distinct. This, together with the fact that $\Lambda(m) = 0$ gives us $\#\operatorname{supp}(m) \geq 2$. Choose any two distinct index pairs (g, i) and (h, j), and we notice that $o_{g,h}(w_{g,i}, w'_{g,i}, w_{h,j}, w'_{h,j})$ is an obstruction, as m is homogeneous. Then we see that for $m' := m - c_{g,i}\operatorname{LC}(g)o_{g,h}(w_{g,i}, w'_{g,i}, w_{h,j}, w'_{h,j})$ we have $\#\operatorname{supp}(m') < \#\operatorname{supp}(m)$. The claim therefore follows by induction over $\#\operatorname{supp}(m)$.

(Compare to [Xiu12, Lemma 3.4.8].) □

Definition 2.16 (lifting)**.** An element $m \in \operatorname{Syz}(\operatorname{LM}(G))$ has a **lifting** in $\operatorname{Syz}(G)$ if there exists $M \in Syz(G)$ such that $\operatorname{LF}(M) = m$. ◁

Lemma 2.17. The set G is a Gröbner basis of (G) if and only if every obstruction of G has a lifting in $\operatorname{Syz}(G)$. ◁

Proof. Let G be a Gröbner basis of I. Let $m \in o(G)$, so $\Lambda(m) = 0$, and as m is an obstruction, we also have $\operatorname{LF}(m) = m$. If $\lambda(m) = 0$, then m is a lifting of itself, so assume $\lambda(m) = 0$. By Proposition 2.9, $\lambda(m)$ has a Gröbner representation, say $\lambda(m) = \sum_i c_i w_i g_i w'_i$ with $c_i \in k^\times$, $w_i, w'_i \in \mathcal{B}$ and $g_i \in G$, and we have $\operatorname{LT}(\lambda(m)) \succeq \operatorname{LT}(w_i g_i w'_i)$ for all i.

Consider $h := \sum_i c_i w_i \epsilon_{g_i} w_i'$, so clearly $\lambda(m) = \lambda(h)$, which implies that $m - h \in \mathrm{Syz}(G)$. By construction we have $\mathrm{LT}(\lambda(m)) = \mathrm{LT}(\lambda(h)) = \deg(h)$. As $\mathrm{LF}(m) = m \in \mathrm{Syz}(\mathrm{LM}(G))$, which means $\Lambda(m) = 0$, the leading terms in the resulting sum of $\lambda(m)$ cancel each other out. This means that we get $\deg(m) \succ \mathrm{LT}(\lambda(m)) = \mathrm{LT}(\lambda(h))$ and therefore $\deg(m) \succ \deg(h)$, so $\mathrm{LF}(m - h) = \mathrm{LF}(m) = m$. This shows that $m - h$ is a lifting of m.

Assume that every obstruction in $o(G)$ has a lifting in $\mathrm{Syz}(G)$. Let $f \in I$, and choose a representation $f = \sum_i c_i w_i g_i w_i'$ with $c_i \in k^\times$, $w_i, w_i' \in \mathcal{B}$ and $g_i \in G$ for all i, such that $\max\{\mathrm{LT}(w_i g_i w_i')\}$ is minimal, which is possible because $\preceq$ is a well order.

Assume towards a contradiction that $\max\{\mathrm{LT}(w_i g_i w_i')\} \succ \mathrm{LT}(f)$, and let $m = \sum_i c_i w_k \epsilon_{g_i} w_i'$, which by construction is an m such that $\lambda(m) = f$ with minimal $\deg(m)$. Also by construction we have $\deg(m) \succ \mathrm{LT}(f) = \mathrm{LT}(\lambda(m))$, which necessarily implies $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}(G))$. By Lemma 2.15, we can find $d_j \in k^\times$, $v_j, v_j' \in \mathcal{B}$ and $m_j \in o(G)$ such that $\mathrm{LF}(m) = \sum_j d_j w_j m_j w_j'$. Choose a lifting $M_j \in \mathrm{Syz}(G)$ for each m_j, so $\mathrm{LF}(M_l) = m_l$, which exist by assumption. As $M_l \in \mathrm{Syz}(G)$, we have $\lambda(m - \sum_j d_j v_j M_j v_j') = \lambda(m)$. But we also have

$$\mathrm{LF}(m) = \sum_j d_j v_j \,\mathrm{LF}(M_j) v_j' = \mathrm{LF}(\sum_i c_j v_j M_j v_j') \;,$$

and therefore $\deg(m - \sum_j d_j v_j M_j v_j') \prec \deg(m)$, therefore contradicting the minimality of $\deg(m)$.

So we must have $\max\{\mathrm{LT}(w_i g_i w_i')\} \preceq \mathrm{LT}(f)$, which means that $\sum_i c_i w_i g_i w_i'$ is a Gröbner representation of f. With Proposition 2.9, we showed that G is a Gröbner basis of I, concluding our proof.

(Compare to [Xiu12, Proposition 3.4.11].) □

Definition 2.18 (S-polynomial)**.** Let A be a k-algebra with multiplicative basis $\mathcal{B}$ and an admissible order, and let $G \subseteq R$ be a finite subset. Let $o_{g,h}(v, v'; w, w') \in o_{g,h}$ be an obstruction. We define the **S-polynomial** of $o = o_{g,h}(v, v'; w, w')$ as

$$S(o) = S_{g,h}(v, v'; w, w') := \lambda(o_{g,h}(v, v'; w, w')) \;.$$

◁

We now give an even better version of Proposition 2.9.

Proposition 2.19. *A finite set $G \subseteq A$ is a Gröbner basis of $I = (G)$ if and only if for every obstruction $o \in o(G)$, the S-polynomial $S(o)$ has a Gröbner representation in terms of G.* ◁

Proof. If G is a Gröbner basis, then Proposition 2.9 immediately gives us that every S-polynomial $S(o) \in I$ for an obstruction $o \in o(G)$ has a Gröbner representation.

Assume now that every S-polynomial $S(o)$ of an obstruction $o \in o(G)$ has a Gröbner representation. By Lemma 2.17, to show that G is a Gröbner basis of I, it suffices to show that each obstruction in $o(G)$ has a lifting in $\mathrm{Syz}(G)$. So let $o = o_{g,h}(w, w', v, v')$ be an obstruction, and let $S(o) = \sum_i c_i w_i g_i w_i'$ be a Gröbner representation of $S(o)$. Let

$M = o - \sum_i c_i w_i \epsilon_{g_i} w_i'$. Since the leading terms of $S(o)$ cancel each other out in the sum, we must have $\mathrm{LT}(w_j g_j w_j) \prec \mathrm{LT}(wgw') = \mathrm{LT}(vhv')$ for all j. This means that we have $\mathrm{LF}(M) = o$, and furthermore $M \in \mathrm{Syz}(G)$ by construction, so M is a lifting of o in $\mathrm{Syz}(G)$.

(Compare to [Xiu12, Proposition 4.1.2].) □

Remark 2.20. In the setting of the commutative polynomial ring $A = k[x_1, \ldots, x_n]$, there is only one S-polynomial we need to consider for a pair of polynomials. For $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{N}_0^{[n]}$ we write $x^\lambda := x^{\lambda_1} \ldots x^{\lambda_n}$. Let $f, g \in A$, we can then write $\mathrm{LT}(f) = x^\alpha$ and $\mathrm{LT}(g) = x^\beta$ for some $\alpha, \beta \in \mathbb{N}_0^{[n]}$. Define $\nu \in \mathbb{N}_0^{[n]}$ by $\nu_i := \min\{\alpha_i, \beta_i\}$, and consider

$$S(f,g) := \frac{1}{\mathrm{LC}(f)} x^{\beta-\nu} \cdot f - \frac{1}{\mathrm{LC}(g)} x^{\alpha-\nu} \cdot g \,,$$

which is the S-polynomial $S(o)$ of the obstruction $o_{f,g}(x^{\beta-\nu}, 1; x^{\alpha-\nu}, 1)$. Every other S-polynomial $S(o')$ of an obstruction $o' \in o(f,g)$ will then just be a multiple of $S(f,g)$. We conclude that $S(f,g)$ reduces to zero with respect to some set G if and only the S-polynomial $S(o')$ of every obstruction $o' \in o(f,g)$ reduces to zero with respect to G. This is **Buchberger's criterion** for commutative polynomials. ◁

We now almost have an algorithm to compute Gröbner bases. For a given set of generators G of an ideal I, we can check if an S-polynomial reduces to 0 if we do the division by G. If no such S-polynomial exists, then by Proposition 2.19 we already have a Gröbner basis. But if S-polynomials exist that don't reduce to 0, then we append them to G, and let's call that set G'. Obviously these S-polynomials and therefore all S-polynomials $S(o)$ for $o \in o(G)$ for reduce to 0 with respect to G'. But this doesn't guarantee that G' isn't a Gröbner basis for I, because for Proposition 2.19 to work, we now have to check the S-polynomials for $o(G')$. So we want to repeat the process until all S-polynomials reduce to 0. This poses two challenges if we want to implement this algorithmically.

1. We have infinitely many S-polynomials that we need to check, even if G is finite.
2. If we assume that we can somehow check all the S-polynomials and we additionally assume that we only append finitely many new S-polynomials, we still have no guarantee that the algorithm terminates.

In the following, we see that we can tackle problem 1. We know of examples where an ideal generated by finitely many elements has an infinite reduced Gröbner basis, so problem 2 cannot be eliminated by technique, but only by changing the circumstances, id est placing restrictions on our multiplicative basis $\mathcal{B}$.

2.5. Buchberger's criterion

What we want to do in the end, is to reduce the amount of S-polynomials we need to check in Proposition 2.19 in such a way that we can possibly algorithmically compute

Gröbner bases. In Remark 2.20, we saw an example for how we can reduce the case of many S-polynomials to a single specific S-polynomial, and we try to now do something similar for the noncommutative case.

Lemma 2.21. Let $o = o_{g,h}(u, w; u', w') \in o(g, h) \subseteq o(G)$ such that its S-polynomial $S(o)$ has a Gröbner representation in therms of G. Then for any $m, n \in \mathcal{B}$, the S-polynomial $S(o')$ of $o' = o_{g,h}(mu, wn; mu', w'n) \in o(g, h)$ also has a Gröbner representation in terms of G. ◁

Proof. We note that $o' = mon$, and therefore if $o = \sum_i c_i v_i g_i v_i'$ is a Gröbner representation, then $o' = \sum_i c_i (mv_i) g_i (v_i' n)$ is a Gröbner representation.
(Compare to [Xiu12, Lemma 4.1.6].) □

With this, our goal is to modify our characterization in Proposition 2.19 in such a way that we only need to check all obstructions of the form

1. $o_{g,h}(1, w; u, 1)$ a "right obstruction in $o(g, h)$",
2. $o_{g,h}(u, 1; 1, w)$, a "left obstruction in $o(g, h)$",
3. $o_{g,h}(1, 1; u, w)$, an "inner center obstruction in $o(g, h)$", and
4. $o_{g,h}(u, w; 1, 1)$, an "outer center obstruction in $o(g, h)$".

There is a bit of a problem in this notation, as 1 is not necessarily an element of $\mathcal{B}$. We could just allow 1, or alternatively, we can choose some $l_{\mathrm{LT}(g)}$, $r_{\mathrm{LT}(g)}$, $l_{\mathrm{LT}(h)}$ or $r_{\mathrm{LT}(h)}$ instead of 1, as described in Proposition 1.6. We will stick to just writing 1, as in the end it won't make a difference, and it is both more pleasing to the eye as well as more similar to the literature.

If $\mathcal{B}$ is infinite, which for instance is the case for path algebras, there are still infinitely many of these obstructions. As an example, for any $b \in \mathcal{B}$, we have that $o_{g,h}(1, b\,\mathrm{LT}(h); \mathrm{LT}(g)b, 1)$ is an obstruction. Luckily, among these we don't need to check all of them for arbitrary $b \in \mathcal{B}$: We can "trim off" b, meaning we set $b = 1$, and then if that S-polynomial $o_{g,h}(1, \mathrm{LT}(h); \mathrm{LT}(g), 1)$ reduces to 0, then all S-polynomials of the form $o_{g,h}(1, b\,\mathrm{LT}(g); \mathrm{LT}(h)b, 1)$ for arbitrary $b \in \mathcal{B}$ reduce to 0 by applying Lemma 2.21 again. But it obviously doesn't suffice to only check $o_{g,h}(1, \mathrm{LT}(h); \mathrm{LT}(g), 1)$ and $o_{g,h}(\mathrm{LT}(h), 1; 1, \mathrm{LT}(g))$ as left and right obstructions, we definitely need to check more. Essentially, we can think of what we need to additionally check as "trimming off" even more off of $\mathrm{LT}(g)$ and $\mathrm{LT}(h)$. This inspires the following definition, which is described in [Gre99, Definition 2.7].

Definition 2.22 (overlap, non-trivial obstruction)**.** Let $b, c \in \mathcal{B}$. We say b and c **overlap** if there exist $u, w \in \mathcal{B}$ such that one of the following conditions hold.

1. $bw = uc \neq 0$ and $b \nmid u$ and $c \nmid w$, "b overlaps on the right with c".
2. $ub = cw \neq 0$ and $b \nmid w$ and $c \nmid u$, "b overlaps on the left with c".

3. $b = ucw$, meaning c divides b,

4. $ubw = c$, meaning b divides b.

Cases 3 and 4 imply $c \mid b$ and $b \mid c$, respectively.

Let $g, h \in G$ and assume that $\mathrm{LT}(g)$ and $\mathrm{LT}(h)$ overlap. Then consider the obstruction $o \in o(g, h)$ as the following for each of the four cases.

1. $o = o_{g,h}(1, w; u, 1)$, a "right obstruction in $o(g, h)$"

2. $o = o_{g,h}(u, 1; 1, w)$, a "left obstruction in $o(g, h)$"

3. $o = o_{g,h}(1, 1; u, w)$, an "inner center obstruction in $o(g, h)$"

4. $o = o_{g,h}(u, w; 1, 1)$, an "outer center obstruction in $o(g, h)$"

The set of all such obstructions in $o(g, h)$, aside from $o_{g,h}(1, 1; 1, 1)$ if $g = h$, is denoted by $O(g, h)$, and the union of all these for $g, h \in G$ is denoted by $O(G)$, and we call them **non-trivial obstructions** of G.

If we have an obstruction of G of the form $o_{g,h}(mu, wn; pu', w'q)$ for a non-trivial obstruction $o_{g,h}(u, w; u'w')$ of G and for $m, n, p, q \in \mathcal{B}$, we say it has an **overlap**.

◁

Remark 2.23. Let A be a path algebra. Definition 2.22 is equivalent to the following. Let $b, c \in \mathcal{B}$. Then b and c overlap at $v \in \mathcal{B}$ if there exist $u, w \in \mathbb{Q}_{\geq 1}$ such that one of the following conditions hold.

1. $b = uv$ and $c = vw$, "b overlaps in v on the right with c".

2. $b = vw$ and $c = uv$, "b overlaps in v on the left with c".

3. $b = uvw$ and $c = v$, "b is contains b".

4. $b = v$ and $c = uvw$, "b is lies inside of c".

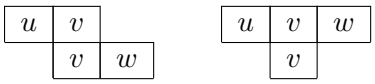


Figure 2.1.: *A visualization for overlaps.*

In this context, the term "overlap" is a bit more intuitive. ◁

Example 2.24. Consider $k\langle x, y\rangle$ and the monomials $x^3y^2x^2$ and x^2y^2x. We have the following overlaps.

$xxxyyxx$	$xxxyyxx$	$xxxyyxx$	$xxxyyxx$
$xxyyx$	$xxyyx$	$xxyyx$	$xxyyx$
center	right	right	left

◁

The question now is if for our characterization in Proposition 2.19 it suffices to check only S-polynomials $s(o)$ for non-trivial obstruction $o \in O(G)$. For path algebras this is exactly the case. Overlaps exactly describe the smallest "building blocks" from which we "construct" all other obstructions that have an overlap (via Lemma 2.21).

We now restrict ourselves to path algebras, so in the following, Q is a quiver and kQ its path algebra. The following results rely on an important lemma that is not necessarily generalizable.

Lemma 2.25. Let $a, b, v \in Q_{\geq 0}$ such that $av = vb$. We can then find $x, y \in Q_{\geq 0}$ and $n \in \mathbb{N}_0$ such that $a = xy$, $b = yx$ and $w = (xy)^n$. ◁

Proof. If one of the a, b or v are in Q_0, then it is clear. Assume therefore that $a, b, v \in Q_{\geq 1}$. Observe that we must have $\ell(a) = \ell(b)$. Now consider $\ell(v) = n\,\ell(a) + r$, where $n \in \mathbb{N}_0$ and $r < \ell(a)$. By induction over n we have $v = a^n x$ with $\ell(x) = r$. With $\ell(x) = r < \ell(a) = \ell(b)$, we have $b = yx$ for some $y \in \mathcal{B}$. Then, since $a^n ax = av = vb = a^n xyx$, we must have $ax = xyx$, and therefore $a = xy$. This concludes the proof.

(Compare to [Coh08, Lemma 1.2].)

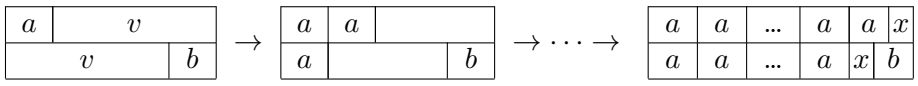


Figure 2.2.: *A visualization for the induction in the proof of Lemma 2.25.*

□

Lemma 2.26. Let $g, h \in kQ$ and assume that $\mathrm{LT}(g)$ and $\mathrm{LT}(h)$ have no overlap. Then the S-polynomial $S(o)$ for any obstruction $o \in o(g, h)$ has a Gröbner representation. ◁

Proof. In path algebras, an obstruction $o \in o(g, h)$ that has no overlap must be either of the form $o_{g,h}(u, v\,\mathrm{LT}(h)w; u\,\mathrm{LT}(g)v, w)$ or $o_{g,h}(u\,\mathrm{LT}(h)v, w; u, v\,\mathrm{LT}(g)w)$ for some $w, v, u \in Q_{\geq 0}$ for some $w, v, u \in Q_{\geq 0}$, and for symmetry reasons it suffices to only consider the former. Furthermore, it also suffices to just check $o_{g,h}(1, v\,\mathrm{LT}(h); \mathrm{LT}(g)v, 1)$, since if we can show it for this case, Lemma 2.21 guarantees us the general case.

Without loss of generality, we can assume that $\mathrm{LC}(g) = \mathrm{LC}(h) = 1$. We calculate a representation of $S(o)$ in terms of g and h as follows. Let $g = \mathrm{LT}(g) + \sum_{j \in J} \lambda_j a_j$ and $h = \mathrm{LT}(h) + \sum_{k \in K} \mu_k b_k$ for $\lambda_j, \mu_k \in k^\times$ and $a_j, b_k \in \mathcal{B}$ for all $j \in J$ and $k \in K$, and for g and h respectively, all basis elements occurring in their expressions are pairwise

distinct. We then have

$$\begin{aligned} S(o) &= gv\,\mathrm{LT}(h) - \mathrm{LT}(g)vh \\ &= gv(h - \sum_{k\in K} \mu_k b_k) - (g - \sum_{j\in J} \lambda_j a_j)vh \\ &= \sum_{k\in K} \mu_k gvb_k - \sum_{j\in J} \lambda_j a_j vh \\ &= \sum_{k\in K'} \mu_k gvb_k - \sum_{j\in J'} \lambda_j a_j vh\ , \end{aligned}$$

where $J' \subseteq J$ are the indices such that $a_j v\,\mathrm{LT}(h) \neq 0$, and analogously for $K' \subseteq K$.

To show that this is in fact a Gröbner representation, by definition, we must show that $\mathrm{LT}(S(o)) \succeq LT(gvb_k) = \mathrm{LT}(g)vb_k$ and $\mathrm{LT}(S(o)) \succeq \mathrm{LT}(a_j vh) = a_j v\,\mathrm{LT}(h)$ for all $k \in K'$ and all $j \in J'$. Let $j' \in J'$ and $k' \in K'$ be the indices such that $\mathrm{LT}(\sum_{j\in J} \lambda_j a_j vh) = a_{j'} v\,\mathrm{LT}(h)$ and $\mathrm{LT}(\sum_{k\in K} \mu_k gvb_k) = \mathrm{LT}(g)vb_{k'}$. Then to show that our representation is a Gröbner representation is to show that either $\mathrm{LT}(S(o)) = a_{j'} v\,\mathrm{LT}(h)$ or $\mathrm{LT}(S(o)) = \mathrm{LT}(g)vb_{k'}$. This in turn is the case if and only if $\lambda_{j'} a_{j'} v\,\mathrm{LT}(h) \neq \mu_{k'}\,\mathrm{LT}(g)vb_{k'}$.

Assume towards a contradiction that we have equality, so $\lambda_{j'} = \mu_{k'}$ and $a_{j'} v\,\mathrm{LT}(h) = \mathrm{LT}(g)vb_{k'}$. Since $a_{j'} \prec \mathrm{LT}(g)$ and $b_{k'} \prec \mathrm{LT}(h)$ (as is true for all a_j and b_k since they are in the support of g and h, respectively), we must have $\mathrm{LT}(g) = a_{j'}u$ and $\mathrm{LT}(h) = wb_{k'}$ for some $u, w \in Q_{\geq q}$. But we then also see that $a_{j'}vwb_{k'} = a_{j'} v\,\mathrm{LT}(h) = \mathrm{LT}(g)vb_{k'} = a_{j'}uvb_{k'}$, and therefore we must have $uv = vw$. By Lemma 2.25, we can find $x, y \in \mathcal{B}$ such that $u = xy$ and $w = yx$. Since $u, w \in Q_{\geq 1}$, we must have $xy, yx \in Q_{\geq 1}$, so $\mathrm{LT}(g)$ and $\mathrm{LT}(h)$ must overlap nontrivially at y if $y \in Q_{\geq 1}$, and they overlap nontrivially at x if $y \in Q_0$, in which case $u = w = x \in Q_{\geq 1}$. But we assumed that $\mathrm{LT}(g)$ and $\mathrm{LT}(h)$ do not overlap, so we have a contradiction. Therefore we must have $\lambda_{j'} a_{j'} v\,\mathrm{LT}(h) \neq \mu_{k'}\,\mathrm{LT}(g)vb_{k'}$, so we do in fact have a Gröbner representation.

(Compare to [Coh08, p. 1.3]).

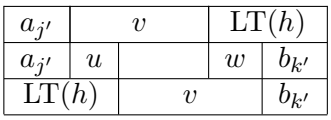


Figure 2.3.: *A visualization for part of the proof of Lemma 2.26.*

□

Now still left are those obstructions of g and h without overlap, but where $\mathrm{LT}(g)$ and $\mathrm{LT}(h)$ do have an overlap. Without some modifications, this case seems to not be easily covered, even for path algebras. So we now restrict to the case of the non-commutative polynomial ring $A = k\langle X\rangle$. In [Xiu12, Lemma 4.1.10], there is a reference to both [Mor94, Lemma 5.4] and to [Coh08, Lemma 1.3], the latter of which also references [Mor94].

Lemma 2.27. If for $g, h \in A = k\langle X \rangle$ all non-trivial obstructions are Gröbner representable, then so are all obstructions in $o(g, h)$. ◁

Proof. See [Coh08, Lemma 1.3]. This proof is rather elaborate and makes use of Lemma 2.26 and Lemma 2.25. One shows that if $\mathrm{LT}(g)$ and $\mathrm{LT}(h)$ have an overlap, then every obstruction of g and h with no overlap can be reduced to the case of an obstruction of g and h with an overlap, which by assumption and together with lemma 2.21 is Gröbner representable. □

We have now covered all cases for S-polynomials, which means that we can simplify Proposition 2.19 to a much simpler version.

Theorem 2.28 (Buchberger's criterion)**.** *A set $G \subseteq A = k\langle X \rangle$ is a Gröbner basis for (G) if and only for every non-trivial obstruction $o \in O(G)$ its S-polynomial $S(o)$ reduces to 0 with respect to G.* ◁

Proof. This is just a result of Proposition 2.19, Lemma 2.26 and Lemma 2.27. □

This is especially helpful, because for a finite set G, the set of non-trivial obstructions is finite. With the division algorithm, we therefore now have a way to algorithmically determine if a set of generators of an ideal is a Gröbner basis or not.

2.6. Buchberger's procedure and interreduction

We now finally arrive at the final form of our algorithm, which is Buchberger's procedure.

Theorem 2.29 (Buchberger's procedure)**.** *Let $A = k\langle X \rangle$ with an admissible order, and let $G \subseteq A$ be a finite subset. If **Buchberger's procedure** terminates with output G', then G' is a Gröbner basis of $I = (G)$. Furthermore, if I has a finite Gröbner basis, then the procedure terminates.* ◁

Algorithm 2 Buchberger's procedure

Input: $G \subseteq A$
Output: $G' \subseteq A$ a Gröbner basis of (G)

```
1: G' ← G
2: FINISH ← False

3: while FINISH = False do
4:     FINISH ← True
5:     for o ∈ O(G') do
6:         if N(S(o); G') ≠ 0 then
7:             G' ← G' ∪ {S(o)}
8:             FINISH ← False
9: return G'
```

Proof. The correctness of the algorithm assuming that it terminates is just an immediate result of Buchberger's criterion (Theorem 2.28). Still to show is that it terminates if there exists a finite Gröbner basis $\tilde{G}$ of I.

Enumerate $G = \{g_1, \dots, g_r\}$, and define $g_n = S(o)$ for $n > r$ successively in the order that we perform the step $G' \leftarrow G' \cup \{S(o)\}$, and consider $G_k = \{g_1, \dots, g_k\}$ and $G_\infty = \{g_n \mid n \in \mathbb{N}_0\}$. The set G_∞ is a Gröbner basis of I by Buchberger's criterion: If $o \in O(G_\infty)$ is an obstruction, then there exists a $k \in \mathbb{N}_{>0}$ such that $o \in O(G_k)$, and if $S(o)$ doesn't reduce to zero with respect to G_k, then it reduces to zero with respect to $G_{k+1} = G_k \cup \{S(o)\}$, in particular with respect to G_∞.

Since G_∞ is a Gröbner basis, we can find for each $g \in \tilde{G}$ a $k' \in \mathbb{N}_{>0}$ and $w_g, w_g' \in \mathcal{B}$ such that $\mathrm{LT}(g) = w_g \,\mathrm{LT}(g_{k'}) w_g'$. Since $\tilde{G}$ is finite, we have a maximal such k'. Therefore $\mathrm{LT}(G_{k'}) = \mathrm{LT}(\tilde{G})$, so $G_{k'}$ is a Gröbner basis, and the algorithm terminates once $G' = G_{k'}$.

(Compare to [Xiu12, Theorem 4.1.4, 4.1.14]) □

Remark 2.30. In Buchberger's procedure (Theorem 2.29), it is also possible to add a break instruction at the end of the if case, but then one has to take care of the order in which the elements $o \in O(G')$ are checked. They have to be checked in such a way that every possible S-polynomial of obstructions in $O(G')$ gets checked eventually in the algorithm This is not automatically given, as $O(G')$, though finite, grows in size every time we append an S-polynomial to G'. ◁

One desire left is that in the end we would like to have a *reduced* Gröbner basis. Given a Gröbner basis, it is indeed possible to remove some kind of a redundancy, while still retaining the property of being a Gröbner basis, and the idea is that we do this until it is no longer possible, after which we retrieve a Gröbner basis. We follow along the lines of [Xiu12, p. 38f], but we can actually generalize to general algebras A.

Definition 2.31 (interreduced)**.** A set $G \subseteq A$ is called **interreduced** if for all $g \in G$, no element in $\mathrm{supp}(g)$ is a member of $\mathrm{LT}(G \setminus \{g\})$. ◁

Proposition 2.32. *A Gröbner basis $G \subseteq A$ of an ideal I is reduced if and only if it is interreduced.* ◁

Proof. Let G be a reduced Gröbner basis, and let $g \in G$. Because we have $g - \mathrm{LT}(g) \in \mathrm{span}(\mathcal{B} \setminus \mathrm{LT}\{I\})$ ((2) in Definition 1.44), any element in $\mathrm{supp}(g) \setminus \{\mathrm{LT}(g)\}$ is not a member of $\mathrm{span}_k(\mathrm{LT}\{I\}) = \mathrm{LT}(G)$ (Remark 1.42), in particular not a member of $\mathrm{LT}(G \setminus \{g\})$. But $\mathrm{LT}(g)$ is also not a member of $\mathrm{LT}(G \setminus \{g\})$, otherwise $\mathrm{LT}\{G\}$ would not be a minimal generating set for $\mathrm{LT}(G)$ ((1) in Definition 1.44). This shows that G is interreduced.

Let G be an interreduced Gröbner basis. We must have that $\mathrm{LT}\{G\}$ is a minimal generating set for $\mathrm{LT}(G)$, because if it weren't, there would be $g, h \in G$ such that $\mathrm{LT}(g) = w\,\mathrm{LT}(h)w'$, which would mean that $\mathrm{LT}(g) \in \mathrm{LT}(G \setminus \{g\})$, contradicting that G was assumed to be interreduced. For $g \in G$, we have by assumption that no element of $\mathrm{supp}(g)$ is a member of $\mathrm{LT}(G \setminus \{g\})$. As all elements in $\mathrm{supp}(g)$ that are not $\mathrm{LT}(g)$ are strictly smaller with respect to $\preceq$, we must have that all elements in $\mathrm{supp}(g - \mathrm{LT}(g))$ are not a member of $\mathrm{LT}(G)$, in other words $g - \mathrm{LT}(g) \in \mathrm{span}(\mathcal{B} \setminus \mathrm{LT}\{I\})$. □

So in order to modify a Gröbner basis into a reduced Gröbner basis, we would like to somehow "interreduce" it.

Lemma 2.33. Let $G \subseteq A \setminus \{0\}$ be a set, and let g' be the remainder of a division by $G \setminus \{g\}$ for some $g \in G$ as in Definition 2.1. Then $G' := (G \setminus \{g\}) \cup \{g'\}$ generates $I = (G)$, and furthermore $\mathrm{LT}(G') = \mathrm{LT}(G)$. ◁

Proof. From the definition of a division (Definition 2.1), we see that $(G') = (G)$ and $\mathrm{LT}(g') \in \mathrm{LT}(G)$, so still to show is $\mathrm{LT}(g) \in \mathrm{LT}(G')$. If $\mathrm{LT}(g) = \mathrm{LT}(g')$, then clearly $\mathrm{LT}(G) = \mathrm{LT}(G')$, so let us now assume $\mathrm{LT}(g) \neq \mathrm{LT}(g')$. We then have $\mathrm{LT}(g) = u\,\mathrm{LT}(h)u'$ for some $h \in G \setminus \{g\}$ by Remark 2.2 item 2, and therefore $\mathrm{LT}(g) \in \mathrm{LT}(G')$. □

Now we present the interreduction algorithm as described in [Xiu12, Theorem 3.2.8].

Proposition 2.34. *The interreduction algorithm takes a finite set G and terminates with output G', an interreduced generating set of $I = (G)$ such that* $\mathrm{LT}(G) = \mathrm{LT}(G')$. ◁

Algorithm 3 interreduction algorithm

Input: finite list $\mathcal{G} = (g_1, \ldots, g_s)$ of elements in $A \setminus \{0\}$
Output: finite list $\mathcal{G}'$ of elements in A such that the underlying set G' is interreduced, and such that $(G) = (G')$ and $\mathrm{LT}(G) = \mathrm{LT}(G')$ for the underlying set G of $\mathcal{G}$

```
finish ← False
while finish = False do
    for i ∈ [s] do
        g'_i ← N(g_i; G \ {0, g_i})
        if g'_i = 0 then
            g_i ← 0                          ▷ removes a redundant generator
        else if g'_i ≠ g_i then              ▷ i.e. if supp(g_i) ∩ LT(G \ {g_i}) ≠ ∅
            g_i ← g'_i
            break                            ▷ i.e. restart the "for" loop at i = 1
        else if i = s then
            finish ← True
G' ← G \ {0}
return G'
```

Proof. We want to show by induction that if for $k \in [s]$, the iteration for $i = k$ of the "for" loop gets reached, then eventually, $i = k + 1$ will be reached in the "for" loop if $i < s$. By this induction, $i = s$ will be eventually reached. Then we show that once $i = s$ is reached, we can guarantee that the last "else if" statement will be reached eventually.

Note that $\mathrm{LT}(g'_i) \preceq \mathrm{LT}(g_i)$ if $g'_i \neq 0$ at any point of the algorithm. Let $k \in [s]$, and consider that we are in the "for" loop at the iteration $i = 1$. Assume that $g'_k \neq 0$ and $g'_k \neq g_k$, as otherwise $i = k + 1$ will be reached immediately, completing the induction

step. This means that we arrive at the break instruction, and we restart the "for" loop at $i = 1$ before i can increase again.

Assume the case that $\mathrm{LT}(g'_k) \prec \mathrm{LT}(g_k)$. By our induction hypothesis, $i = k$ will be reached again (not necessarily in the next "for" loop, but eventually). Therefore if again $g'_k = 0$ or $g'_k = g_k$ (note that these are new g_k and g'_k), either case we will result in reaching $i = k + 1$, completing the induction step. So let's again assume $g'_k \neq 0$ and $g'_k \neq g_k$, meaning we again have $\mathrm{LT}(g'_k) \prec \mathrm{LT}(g_k)$. We now reached the same situation as the one we started with. Since we have a well order, the sequence of cases leading up to this situation can only repeat finitely many times until we eventually get to the case $\mathrm{LT}(g'_k) = \mathrm{LT}(g_k)$.

Assume now the case that $\mathrm{LT}(g'_k) = \mathrm{LT}(g_k)$. As we are currently in the case that $i = k$, it must be that for all $j \in [k-1]$, either $g_j = 0$ or $\mathrm{N}(g_j; \mathcal{G} \setminus \{0, g_j\}) = g_j$. But as $\mathrm{LT}(g'_k) = \mathrm{LT}(g_k)$, we must also have $g_j = 0$ or $\mathrm{N}(g_j; (\mathcal{G} \setminus \{0, g_j, g_k\}) \cup \{g'_k\}) = g_j$ for all $j \in [k-1]$. As we assumed that $g'_k \neq 0$ and $g'_k \neq g_k$, we set $g_k \leftarrow g'_k$, and we break and restart the "for" loop at $i = 1$. With what we just showed, in this next "for" loop, for the iterations $i \in [k-1]$, the case $g'_i \neq 0$ and $g'_i \neq g_i$ will not be fulfilled. Therefore we arrive at iteration $i = k$ again, but with none of the g_j for $j \in [k-1]$ being different from what they were at the previous time we considered the iteration at $i = k$. The only thing that changed is g_k, and therefore we now have the case $g'_k = \mathrm{N}(g_k; \mathcal{G} \setminus \{0, g_k\}) = g_k$. If $k = s$, the algorithm terminates, and otherwise we reach the next iteration $i = k + 1$.

The algorithm returns an interreduced set since for all $g \in G'$ we have $\mathrm{N}(g; \mathcal{G}') = g$ by construction of the algorithm, and by Lemma 2.33 we have $(G) = (G')$ and $\mathrm{LT}(G) = \mathrm{LT}(G')$ as desired. □

Corollary 2.35. *If G is a finite Gröbner basis of an ideal $I \subseteq A$, the interreduction algorithm then returns a finite reduced Gröbner basis G' of I.* ◁

Example 2.36. 1. In this example, we will demonstrate how in the noncommutative case, even a principal ideal might not have a finite Gröbner basis.

Consider $A = k\langle x, y\rangle$ with admissible order $\preceq = \preceq_{\texttt{Dp}}$ and the ideal $I = (G)$ for $G = \{x^2 - xy\}$. The set G is not a Gröbner basis of I: We have $f = (x^2 - xy)(y - x) + x(x^2 - xy) = xyx - xy^2 \in I$, but $\mathrm{LT}(f) = xyx \notin \mathrm{LT}(G)$. Let us compute a Gröbner basis in SINGULAR.

```
> LIB "freegb.lib";
> ring r = 0,(x,y),Dp;
> def A = freeAlgebra(r,4);
> setring A;
> ideal I = x*x - x*y;
> std(I);

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

We notice that the outputted set, call it F, is actually not a Gröbner basis for I: For $g := (x^2 - xy)(y^2 - yx) + (xy)(x^2 - xy) = xy^3x - xy^4 \in I$, we clearly have $\mathrm{LT}(g) = xy^3x \notin \mathrm{LT}(F)$. The polynomial g is of degree 5, but we chose 4 as our degree bound, so SINGULAR only computed elements of the Gröbner basis up to degree 4. Let us increase the degree bound.

```
> def A = freeAlgebra(r,20);
> setring A;
> ideal I = x*x - x*y;
> std(I);

_[1]=x*x-x*y
_[2]=x*y*x-x*y*y
_[3]=x*y*y*x-x*y*y*y
_[4]=x*y*y*y*x-x*y*y*y*y
_[5]=x*y*y*y*y*x-x*y*y*y*y*y
_[6]=x*y*y*y*y*y*x-x*y*y*y*y*y*y
_[7]=x*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y
_[8]=x*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y
_[9]=x*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y
_[10]=x*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y
_[11]=x*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y*y
_[12]=x*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y*y*y
_[13]=x*y*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y*y*y*y
_[14]=x*y*y*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y*y*y*y
*y*y
_[15]=x*y*y*y*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y*y*y
*y*y*y*y
_[16]=x*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y*y
*y*y*y*y*y*y
_[17]=x*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y*y
*y*y*y*y*y*y*y
_[18]=x*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y*y
*y*y*y*y*y*y*y*y*y
_[19]=x*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*y*x-x*y*y*y*y*y*y*y*y
*y*y*y*y*y*y*y*y*y*y
```

We notice a pattern, and it seems like $\{xy^ix - xy^{i+1} \mid i \in \mathbb{N}_0\}$ is a Gröbner basis of I. It indeed can be shown that this is the reduced Gröbner basis of I, which is proven in [GMU98, Proposition 3.1].

2. We will now present a computation of a reduced Gröbner basis, step by step, while having SINGULAR take care of the division.

   Consider $A = k\langle x, y\rangle$ with admissible order $\preceq_{\texttt{Dp}}$, and the ideal $I = (x^2y + x, yx + y)$.

   ```
   > LIB "freegb.lib";
   ```

```
> ring r = 0,(x,y),Dp;
> def A = freeAlgebra(r,20);
> setring A;
> ideal I = x*x*y + x, y*x +y;
> I;

I[1]=x*x*y+x
I[2]=y*x+y
```

Let us now reduce all nontrivial S-polynomials with respect to I.

```
> reduce(y*I[1] - I[2]*x*y,I);
> reduce(I[1]*x - x*x*I[2],I);

y*y-y
x*x+x
```

We now append these remainders.

```
> I = I, y*y-y, x*x+x;;
> I;

I[1]=x*x*y+x
I[2]=y*x+y
I[3]=y*y-y
I[4]=x*x+x
```

Nontrivial obstructions of `I[1]` and `I[2]` have already been checked in the previous step, and by having the remainders added to our list of generators of I, these S-polynomials will now reduce to 0. We also notice that `I[3]` and `I[4]` don't have a nontrivial obstruction. We therefore now have to check the ones of `I[1]` and `I[3]`, of `I[1]` and `I[4]`, of `I[2]` and `I[3]`, and of `I[2]` and `I[4]`.

```
> reduce(I[1]*y - x*x*I[3],I);
> reduce(I[1] - I[4]*y,I);
> reduce(x*I[1] - I[4]*x*y,I);
> reduce(y*I[2] - I[3]*x,I);
> reduce(I[2]*x - y*I[3],I);
> reduce(I[2]*x - y*I[4],I);

0
-x*y+x
x*y-x
0
0
0

> I = I, x*y-x;;
> I;
```

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

As $-xy + x$ and $xy - x$ are scalar multiples of each other, we only added $xy - x$ to our list of generators. Let us again check all nontrivial S-polynomials that we haven't checked yet.

```
> reduce(I[1]-x*I[5],I);
> reduce(I[2]*y-y*I[5],I);
> reduce(x*I[2]-I[5]*x,I);
> reduce(x*I[3]-I[5]*y,I);
> reduce(I[4]*y-x*I[5],I);

0
0
0
0
0
```

By Buchberger's criterion (Theorem 2.28), the resulting set we computed $\{x^2y + x, yx + y, y^2 - y, x^2 + x, xy - x\}$ is a Gröbner basis of I.

Let us now modify this set into an interreduced set of generators as in Proposition 2.34, turning it into a reduced Gröbner basis.

```
> ideal J = I[2],I[3],I[4],I[5];
> reduce(I[1],J);

0

> I[1] = 0;
> ideal J =  I[1],I[3],I[4],I[5];
> reduce(I[2],J);

y*x+y

> ideal J =  I[1],I[2],I[4],I[5];
> reduce(I[3],J);

y*y-y

> ideal J =  I[1],I[2],I[3],I[5];
> reduce(I[4],J);

x*x+x

> ideal J =  I[1],I[2],I[3],I[4];
> reduce(I[5],J);
```

```
x*y-x
```

In the first step, we had $\texttt{I[1]}' = 0$, so we set `I[1] = 0` and continue. In every other step, for each $i = 2, 3, 4, 5$, we have $\texttt{I[i]}' = \texttt{I[i]}$, so we do nothing and continue in each step. We then reach the end of the loop, so we are done, and our result is that $G' = \{yx + y, y^2 - y, x^2 + x, xy - x\}$ is an interreduced set, and therefore a reduced Gröbner basis. In this case, none of the polynomials get modified, only the first polynomial gets removed. Let us now check what the implemented function `std` in SINGULAR computes as a reduced Gröbner basis, which should give us the same result if we did everything correctly.

```
> ideal I = x*x*y + x, y*x +y;
> std(I);

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

So we indeed performed our calculation for the Gröbner basis correctly.

3. Let us now see an example of a Gröbner basis that is not a reduced Gröbner basis, where finding the reduced Gröbner basis consists of more than just removing redundant generators from the nonreduced Gröbner basis.

   Let again $A = k\langle x, y\rangle$ with admissible order $\preceq = \preceq_{\texttt{Dp}}$, and consider the ideal J generated by the set $\{x^2 + xy, xy + y^2, y^2x + y^3\}$.

```
> ring r = 0,(x,y),Dp;
> def A = freeAlgebra(r,20);
> setring A;
> ideal J = x*x + x*y, x*y + y*y, y*y*x+y*y*y;
> J;

J[1]=x*x+x*y
J[2]=x*y+y*y
J[3]=y*y*x+y*y*y
```

   Let us first convince ourselves that this is a Gröbner basis, by again checking that all nontrivial S-polynomials reduce to 0.

```
> reduce(J[1]*y - x*J[2],J);
> reduce(y*y*J[1] - J[3]*x,J);
> reduce(y*y*J[2] - J[3]*y,J);
> reduce(J[2]*y*x - x*J[3],J);

0
0
0
0
```

We can already see that we have $xy \in \text{supp}(\texttt{J[1]})$ and $xy \in \text{LT}(G \setminus \{\texttt{J[1]}\})$, as $\text{LT}(\texttt{J[2]}) = xy$. Let us now perform the interreduction algorithm by hand as in Proposition 2.34.

```
> ideal K = J[2],J[3];
> reduce(J[1],K);

x*x-y*y
```

This is not equal to `J[1]`, so we replace `J[1]` by $x^2 - y^2$ and start again.

```
> J[1] = x*x-y*y;
> J;

J[1]=x*x-y*y
J[2]=x*y+y*y
J[3]=y*y*x+y*y*y

> ideal K = J[2],J[3];
> reduce(J[1],K);

x*x-y*y

> ideal K = J[1],J[3];
> reduce(J[2],K);

x*y+y*y

> ideal K = J[1],J[2];
> reduce(J[3],K);

y*y*x+y*y*y
```

For every $i = 1, 2, 3$ we computed $\texttt{J[i]}' = \texttt{J[i]}$, which means that we are done and get an interreduced Gröbner basis, meaning $\{x^2 - y^2, xy + y^2, y^2x + y^3\}$ is the reduced Gröbner basis of J. Let us again check if SINGULAR agrees with us.

```
> ideal J = x*x + x*y, x*y + y*y, y*y*x+y*y*y;
> std(J);

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

This confirms that we did everything correctly.

4. In this example, we shall see how choosing different orderings can lead to different Gröbner bases. Consider $A = k\langle x, y, z\rangle$, and the ideal I generated by $\{xz^2 + x, zyx - 2x^2 + y\}$. Let us compute a Gröbner basis with respect to the ordering `Dp`.

```
> LIB "freegb.lib";
> ring r = 0,(x,y,z),Dp;
> def A = freeAlgebra(r,40);
> setring A;
> ideal I = x*z*z + x, z*y*x - 2x*x+y;
> std(I);

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

Now let us see what happens when we calculate the Gröbner basis of the same ideal I, but with order `Wp(1,4,2)`, meaning x has weight 1, y has weight 4, and z has weight 2.

```
> ring r = 0,(x,y,z),Wp(1,4,2);
> def A = freeAlgebra(r,40);
> setring A;
> ideal I = x*z*z + x, z*y*x - 2x*x+y;
> std(I);

_[1]=x*z*z+x
_[2]=z*y*x+y-2*x*x
_[3]=x*z*y-x*y*x-2*x*z*x*x
_[4]=x*y*x*x+2*x*z*x*x*x+x*y-2*x*x*x
_[5]=y*z*z+y
_[6]=y*z*y-y*y*x-2*y*z*x*x
_[7]=y*y*x*x+2*y*z*x*x*x+y*y-2*y*x*x
```

As we can see, not only are the generators different, but also the number of generators.

◁

2.7. Further considerations for the general case

One step to make things simpler that [Gre99] does, is assure that the leading terms are pairwise not divisible by one another, so no center obstructions will exist. If this is not the case, we can modify our generators in such a way that no center obstructions exist, but they still generate the same ideal.

Definition 2.37 (tip reduced)**.** A set $G \subseteq A$ is called **tip reduced** if for all $g, h \in G$ with $g \neq h$ we have $\mathrm{LT}(g) \nmid \mathrm{LT}(h)$. ◁

Proposition 2.38 (tip reduction)**.** *Let $G \subseteq A$ be a finite set. If there exist $g, h \in G$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(h)$, say via $u\,\mathrm{LT}(g)w = \mathrm{LT}(h)$, consider the set where we replace*

in G the element h by $h' = h - \frac{\mathrm{LT}(h)}{\mathrm{LT}(g)} ugw$, meaning $G' = (G \setminus \{h\}) \cup \{h'\}$. Repeat this process until no two such elements can be found. This process will always terminate after finitely many steps and yield a generating set for $I = (G)$ that is tip reduced.

Algorithm 4 tip reduction

Input: $G \subseteq A$ finite
Output: $G' \subseteq A$ tip reduced such that $(G') = (G)$

```
1: OCCUR ← True
2: while OCCUR do
3:     OCCUR ← False
4:     for g ∈ G' do
5:         for h ∈ G' do
6:             if ∃u, w ∈ B: u LT(g)w = LT(h) then
7:                 OCCUR ← True
8:                 G' ← (G' \ {h}) ∪ {h − (LT(h)/LT(g)) ugw}
9:                 break
10:        if OCCUR then
11:            break
12: return G'
```

◁

Proof (sketch). That G' generates $I = (G)$ is clear, so after repeating this finitely many times, the resulting set will also generate I. The process must terminate, as our admissible order is a well-order and we have $h' \prec h$.
(Compare to [Gre99, p. 41].) □

There is a version of Buchberger's criterion that applies to any algebra A with multiplicative basis and an admissible order. We shall briefly discuss these scenarios, following along the lines of [Gre99, chapter 2.3]. For this, we must introduce the concept of uniformity.

Definition 2.39 (uniformity)**.** An element $r \in A$ is called left **uniform** if for all $c \in B$ we either have $c \cdot b = 0$ for all $b \in \mathrm{supp}(r)$ or $c \cdot b \neq 0$ for all $b \in \mathrm{supp}(r)$. ◁

Let $f = \sum_i \lambda_i b_i$ be an element in a path algebra with $\lambda_i \in k^\times$ and pairwise distinct $b_i \in \mathcal{B}$. Then f is left uniform if and only if $s(b_i) = s(b_j)$ for all i and j. We can write any such element as a sum of uniform elements, namely

$$f = 1 \cdot f = \sum_{v \in Q_0} vf = \sum_{v \in Q_0} \sum_{s(b_i) = v} \lambda_i b_i \ .$$

Since each of the vf is in the ideal generated by f, any ideal can be generated by uniform elements.

We then have the following version of Buchberger's criterion, which is proven for path algebras in [Gre99, Theorem 2.3].

Theorem 2.40. *A uniform and tip reduced set $G \subseteq A = k\langle X \rangle$ is a Gröbner basis for (G) if and only for every non-trivial obstruction $o \in O(G)$ its S-polynomial $S(o)$ reduces to 0 with respect to G.* $\lhd$

3. G-Algebras

In our discussion of noncommutative Gröbner bases, our main hindrance was that our k-algebra was not Noetherian in general, meaning that ideals are not necessarily always finitely generated, and even if they are, we cannot guarantee a finite Gröbner basis. There are examples of noncommutative k-algebras that are Noetherian, for example universal enveloping algebras $\mathrm{U}(\mathfrak{g})$ of finite dimensional Lie algebras $\mathfrak{g}$, where we have the following nice properties.

- The Poincaré-Birkhoff-Witt (PBW) theorem: For a basis $\{x_1, \ldots, x_n\}$ of $\mathfrak{g}$, the set $\{x_1^{\lambda_1} \ldots x_n^{\lambda_n} \mid \lambda_i \in \mathbb{N}_0\}$ is a k-basis of $\mathrm{U}(\mathfrak{g})$.
- It is "close to commutative": For $i < j$ we have $x_j \cdot x_i = x_i \cdot x_j - [x_i, x_j]$ due to $[x_i, x_j] = x_i \cdot x_j - x_j \cdot x_i$ as per definition. Furthermore $[x_i, x_j]$ has degree 1 and $x_j x_i$ and $x_i x_j$ have degree 2 in $k\langle x_1, \ldots, x_n\rangle$.
- $\mathrm{U}(\mathfrak{g})$ is left and right Noetherian.

We can define a notion of algebras that have these properties and generalize universal enveloping algebras. These algebras are called G-algebras, and it is possible to develop Gröbner basis theory in such algebras. This was first comprehensively introduced in [Lev05b], and these concepts were also implemented in SINGULAR. We will briefly go over the main results and check some examples.

3.1. Gröbner bases and the non-degeneracy conditions

Definition 3.1 (G-algebra, non-degeneracy conditions)**.** Consider $A = k\langle x_1, \ldots, x_n\rangle$ and let $d_{i,j} \in A$ and $c_{i,j} \in k^\times$ for $0 \leq i < j \leq n$. We now define the polynomials

$$f_{j,i} = x_j x_i - (c_{i,j} \cdot x_i x_j + d_{i,j}) \,,$$

and F as the set of all $f_{j,i}$. We furthermore define the **non-degeneracy conditions**

$$\begin{aligned} \mathrm{NDC}_{i,j,k} = \quad & c_{i,k}c_{j,k} \cdot d_{i,j}x_k - x_k d_{i,j} \\ + \quad & c_{j,k} \cdot x_j d_{i,k} - c_{i,j} \cdot d_{i,k} x_j \\ + \quad & d_{j,k}x_i - c_{i,j}c_{i,k} \cdot x_i d_{j,k} \end{aligned}$$

for $0 \leq i < j < k \leq n$.

Let furthermore $\preceq$ be an admissible order on $k\langle x_1, \ldots, x_n\rangle$ such that

$$\mathrm{LT}(f_{j,i}) = x_j x_i \text{ and } \mathrm{LT}(d_{i,j}) \prec x_i x_j \text{ for all } 0 \leq i < j \leq n \,.$$

If then $\mathrm{N}(\mathrm{NDC}_{i,j,k}; F) = 0$ for all $0 \leq i < j < k \leq n$, then we call $R = A/(F)$ a **G-algebra**. ◁

Remark 3.2. Studying $k\langle x_1, \ldots, x_n\rangle/(F)$, we can without loss of generality assume that the $d_{i,j} \in \operatorname{span}_k\{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbb{N}_0\}$: If $x_k x_l$ occurs in $\operatorname{supp}(d_{i,j})$ such that $k > l$, we can then substitute it by $c_{j,k} x_l x_k + d_{l,k}$. Doing this over and over, this process must terminate, as our admissible order is a well order. ◁

Let $\mathfrak{g}$ be a finite dimensional Lie algebra. If $\{x_1, \ldots, x_n\} \subseteq \mathfrak{g}$ is a k-basis of $\mathfrak{g}$, then the universal enveloping algebra $\mathrm{U}(\mathfrak{g})$ of $\mathfrak{g}$ is given by

$$\mathrm{U}(\mathfrak{g}) = k\langle x_1, \ldots, x_n\rangle/([x_i, x_j] - (x_i x_j - x_j x_i) \mid i, j \in [n]) \,.$$

We then have

$$\begin{aligned} [x_i, x_j] &= x_i x_j - x_j x_i \text{ , and therefore} \\ x_j x_i &= x_i x_j - [x_i, x_j] \end{aligned}$$

in $\mathrm{U}(\mathfrak{g})$ for all $i, j \in [n]$, in particular for all $1 \leq i < j \leq n$. Looking at Definition 3.1, we can define $f_{j,i} := x_j x_i - (c_{i,j} x_i x_j + d_{i,j})$ for $1 \leq i \leq j \leq n$ with

$$\begin{aligned} c_{i,j} &= 1 \\ d_{i,j} &= -[x_i, x_j] \,, \end{aligned}$$

and we notice that $\mathrm{U}(\mathfrak{g}) \cong k\langle x_1, \ldots, x_n\rangle/(F)$, where F is the set of all $f_{j,i}$. The non-degeneracy conditions are fulfilled as a result of the Jacobian identity, so in some sense the non-degeneracy conditions are a generalization of the Jacobian identity. It is then not surprising that PBW basis theorem generalizes to G-algebras, which is the following theorem.

Theorem 3.3. *In the setting of Definition 3.1, the following are equivalent.*

1. *The set F is a Gröbner basis for (F).*
2. *For all $0 \leq i < j < k \leq n$ we have $\mathrm{N}(\mathrm{NDC}_{i,j,k}; F) = 0$ (for any normal remainder).*
3. *The k-algebra $k\langle x_1, \ldots, x_n\rangle/(F)$ has a PBW basis*

◁

Proof. See [Lev05b, Theorem 2.3]. □

Remark 3.4. Once we fix an order for the generating variables $x_1 \prec \cdots \prec x_n$, it doesn't matter what admissible order we choose on $k\langle x_1, \ldots, x_n\rangle$ that fulfills the requirements in Definition 3.1, the resulting PBW basis will always be the same. ◁

3.2. Checking the non-degeneracy conditions in Singular

Let us now look at $\mathrm{U}(\mathfrak{sl}_2)$, which we want to define and work with in SINGULAR.

Example 3.5. The universal enveloping algebra $\mathrm{U}(\mathfrak{sl}_2)$ of $\mathfrak{sl}_2$ is defined by the relations

$$\begin{aligned} f_{2,1} &= fe - (ef - h) \\ f_{3,1} &= he - (eh + 2e) \\ f_{3,2} &= hf - (fh - 2f) \end{aligned}$$

in $k\langle e, f, h\rangle$, where we named the polynomials as in Definition 3.1. We also know that this is a Gröbner basis for the ideal it generates, as the non-degeneracy conditions hold.

We now have the following values for our $c_{i,j}$ and $d_{i,j}$.

$$\begin{aligned} c_{1,2} = c_{1,3} = c_{2,3} &= 1 \\ d_{1,2} &= -h \\ d_{1,3} &= 2e \\ d_{2,3} &= -2f \end{aligned}$$

As mentioned in Remark 3.2, the $d_{i,j}$ can be chosen to be in $\{x_1^{\lambda_1} \cdot \cdots \cdot x_n^{\lambda_n} \mid \lambda_i \in \mathbb{N}_0\}$. Indeed, internally, SINGULAR requires the elements $d_{i,j}$ to be in $k[x_1, \ldots, x_n]$. For universal enveloping algebras, and therefore in our example, this is not a problem as the $d_{i,j}$ are of degree 1.

To define a G-algebra, we can input these into matrices `C` and `D`.

```
> ring r = 0,(e,f,h),Dp;
> setring r;
> matrix D[3][3];  // initialize a 3x3 matrix
> D[1,2]=-h; D[1,3]=2e; D[2,3]=-2f;  // input values
```

We can now define our G-algebra with the function `nc_algebra`, where we must input our matrices `C` and `D`. The function `nc_algebra` will only consider the strict upper entries, and if we input a value instead of a matrix, SINGULAR will use that value for every entry it expects. This means that to define our G-algebra and work with it, we can now input the following.

```
> LIB "freegb.lib";
> def A = nc_algebra(1,D);
> setring A;
> A;

// coefficients: QQ
// number of vars : 3
//        block   1 : ordering Dp
//                  : names    e f h
//        block   2 : ordering C
// noncommutative relations:
//    fe=ef-h
//    he=eh+2e
//    hf=fh-2f
```

There is one tricky detail with SINGULAR that should be pointed out. So far, we have only typed in data of elements in $k[e, f, h]$, as is expected by SINGULAR. When we work in the G-algebra `A`, we must write `*` between variables. For instance, if we have the element hfe, `hfe` will be treated as residing in $k[e, f, h]$, so we shall type in `h*f*e`. The output will always be displayed in $k[e, f, h]$.

```
> hfe;
efh
> h*f*e;
efh-h2
```

What the `*` operation does is replace $x_j x_i$ by $x_i x_j + d_{i,j}$ if $i < j$. With the same argument as in Remark 3.2, as $d_{i,j}$ is strictly smaller than $x_j x_i$, this process will stop after finitely many steps, since we have an admissible order. After this process has ended, the final output will be presented in terms of $\{x_1^{\lambda_1} \cdot \dots \cdot x_n^{\lambda_n} \mid \lambda_i \in \mathbb{N}_0\}$. Via the PBW theorem this is a basis, meaning that this operation must be associative by uniqueness.

```
> f*f*e*h;
ef2h-2fh2+2fh
> e*f*e*h;
e2fh-eh2
> f*f*e*h*e*f*e*h;
e3f3h2+2e3f3h-7e2f2h3-8e2f2h2+10efh4+12e2f2h+14efh3-2h5-12efh2-6h4-4h3
> (ef2h-2fh2+2fh)*(e2fh-eh2);
e3f3h2+2e3f3h-7e2f2h3-8e2f2h2+10efh4+12e2f2h+14efh3-2h5-12efh2-6h4-4h3
> f*f*e*(eh+2e)*f*e*h;
e3f3h2+2e3f3h-7e2f2h3-8e2f2h2+10efh4+12e2f2h+14efh3-2h5-12efh2-6h4-4h3
```

◁

Let us see another example, a Weyl algebra.

Example 3.6 (Weyl Algebra)**.** We shall present the example of the Weyl algebra. The Weyl algebra is important in physics, especially in quantum mechanics, where it describes the space of linear operators on the Hilbert space of L^2 generated by the position operators and momentum operators. We fix $n \in \mathbb{N}_{>0}$ and for each $i \in [n]$ we have generators x_i and ∂_i, subject to the following relations:

- $\partial_i x_i = x_i \partial_i + 1$, the chain rule,
- $\partial_i \partial_j = \partial_j \partial_i$, Schwarz's theorem, and
- $x_i x_j = x_j x_i$, commutativity.

If we order our elements $x_1 \prec \dots \prec x_n \prec \partial_1 \prec \dots \prec \partial_n$ and then choose the left degree lexicographic order on $k\langle x_1, \dots, x_n, \partial_{x_1}, \dots, \partial_{x_n}\rangle$, defining the $f_{j,i}$ according to those equations fulfills our requirements.

Let us implement this in SINGULAR with $n = 3$, and check if the non-degeneracy conditions hold. We have the values $c_{i,j} = 1$ for all i, j, $d_{1,4} = d_{2,5} = d_{3,6} = 1$, and $d_{i,j} = 0$ for all other i, j. We can now input our data into SINGULAR.

```
> LIB "freegb.lib";
> ring r = 0,(x,y,z,dx,dy,dz),dp;
> setring r;
> matrix D[6][6];
> D[1,4] = 1; D[2,5] = 1; D[3,6] = 1;
> def A = nc_algebra(1,D);
> setring A;
> A;

// coefficients: QQ
// number of vars : 6
//        block   1 : ordering Dp
//                  : names    x y z dx dy dz
//        block   2 : ordering C
// noncommutative relations:
//    dxx=x*dx+1
//    dyy=y*dy+1
//    dzz=z*dz+1
```

The function `nc_algebra` expects two matrices. The first argument is the matrix C obtained from the $c_{i,j}$ and the second argument is the matrix obtained from the $d_{i,j}$, and the function only regards values for $i < j$, Note that when we initialize the matrix `D`, all values are 0. SINGULAR has the function `ndcond()` which checks if the non-degeneracy conditions hold.

```
> printlevel = 1;   // verbose output
> ndcond();

Processing degree : 1
1 . 2 . 3 .
1 . 2 . 4 .
1 . 2 . 5 .
1 . 2 . 6 .
1 . 3 . 4 .
1 . 3 . 5 .
1 . 3 . 6 .
1 . 4 . 5 .
1 . 4 . 6 .
1 . 5 . 6 .
2 . 3 . 4 .
2 . 3 . 5 .
```

```
2 . 3 . 6 .
2 . 4 . 5 .
2 . 4 . 6 .
2 . 5 . 6 .
3 . 4 . 5 .
3 . 4 . 6 .
3 . 5 . 6 .
4 . 5 . 6 .
done
_[1]=0
```

So we indeed have a G-algebra. The output indicates which non-degeneracy condition $\mathrm{NDC}_{i,j,k}$ it is checking.

If we change our relations, we can see an example that isn't a G-algebra, and SINGULAR will inform which non-degeneracy condition $\mathrm{NDC}_{i,j,k}$ is not fulfilled.

```
ring r = 0,(x,y,z,dx,dy,dz),Dp;
setring r;
matrix D[6][6];
D[1,4] = dz*z+x; D[2,5] = 1; D[3,6] = 1;
def A = nc_algebra(1,D);
setring A;
A;

// coefficients: QQ
// number of vars : 6
//        block   1 : ordering Dp
//                  : names    x y z dx dy dz
//        block   2 : ordering C
// noncommutative relations:
//    dxx=x*dx+z*dz+x
//    dyy=y*dy+1
//    dzz=z*dz+1

> ndcond();

Processing degree : 1
1 . 2 . 3 .
1 . 2 . 4 .
1 . 2 . 5 .
1 . 2 . 6 .
1 . 3 . 4 .
failed: -z
1 . 3 . 5 .
1 . 3 . 6 .
```

```
1 . 4 . 5 .
1 . 4 . 6 .
failed: -dz
1 . 5 . 6 .
2 . 3 . 4 .
2 . 3 . 5 .
2 . 3 . 6 .
2 . 4 . 5 .
2 . 4 . 6 .
2 . 5 . 6 .
3 . 4 . 5 .
3 . 4 . 6 .
3 . 5 . 6 .
4 . 5 . 6 .
done
_[1]=-z
_[2]=-dz
```

We also see in this example how the associativity of * can go wrong when we don't have a PBW basis. Different orders in which we perform the operation as described in Remark 3.2 can lead to different results.

```
> (dz*dx)*x;
> dz*(dx*x);

x*dx*dz+z*dz^2+x*dz
x*dx*dz+z*dz^2+x*dz+dz
```

◁

3.3. Gröbner bases in G-algebras

The PBW basis for a G-algebra is not a multiplicative basis, so we cannot apply our theory of Gröbner bases from before to them as is. Still, it is indeed possible to also develop a theory of Gröbner bases for G-algebras, which resembles the theory o Gröbner bases in commutative k-algebras. We will briefly discuss what is possible. In the following, A will denote a G-algebra presented as $k\langle x_1, \dots, x_n\rangle/(F)$ as in Definition 3.1 with PBW basis $\{x_1^{\lambda_1} \cdot \dots \cdot x_n^{\lambda_n} \mid \lambda_i \in \mathbb{N}_0\}$. An ideal $I \subseteq A$ will refer to a left ideal in A, and we write ${}_A(M)$ for the left ideal generated by M in A. Let furthermore $\preceq$ be an admissible order on $\langle x_1, \dots, x_n\rangle \subseteq k[x_1, \dots, x_n]$. The set $\mathcal{B}$ will refer to the PBW basis of A.

The underlying vector spaces of A and $k[x_1, \dots, x_n]$ are the same, and $\mathcal{B} = [x_1, \dots, x_n]$ as sets, so $\preceq$ is a well order on $\mathcal{B}$, but we can't call quite it an admissible order, since in A, the set $\mathcal{B} \cup \{0\}$ is not closed under multiplication.

We will now define alternate versions of the terminology in Gröbner basis theory for G-algebras, as is described in [Lev05a, Definition 1.8].

Definition 3.7. Let $G \subseteq A$ be a subset, $I \subseteq A$ be a left ideal, and let $f, g \in G$.

- We define $\mathrm{LT}(f)$, $\mathrm{LC}(f)$, $\mathrm{LM}(f)$ to be just as in Definition 1.41, where we view $f \in k[x_1, \ldots, x_n]$ to be a commutative polynomial. We also define $\mathrm{LT}\{G\}$ and $\mathrm{LT}(F)$ by viewing $F \subseteq k[x_1, \ldots, x_n]$.
- We call G a left **Gröbner basis** of I if ${}_A(G) = I$ and if $\mathrm{LT}(G) = \mathrm{LT}(I)$, in other words, by Proposition 1.45, for every $f \in I$ there exists $g \in G$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(f)$ in $k[x_1, \ldots, x_n]$.
- We define the **S-polynomial** $S(f, g) \in A$ as in Remark 2.20.
- We call $\mathrm{N}(\bullet; G) \colon A \to A$ a **left normal form** with respect to G, if
  - $\mathrm{N}(y; G) = 0$ for $y = 0$
  - $\mathrm{N}(y; G) \neq 0 \implies \mathrm{LT}(\mathrm{N}(y; G)) \notin \mathrm{LT}(G)$, and
  - $y - \mathrm{N}(y; G) \in {}_A(G)$.

  for all $y \in A$.
- A representation $y = \sum_{g \in G} a_g \cdot g$ for $a_g \in A$ is called a **standard left representation** of f with respect to G if $\mathrm{LT}(y) \geq \mathrm{LT}(a_g g)$ for all $g \in G$.

(Compare to [Lev05a, Definition 1.8].) ◁

There indeed always is a normal form with respect to G, which is presented in [Lev05a, Algorithm 1.1, p.51]. We now present a version of Buchberger's criterion for G-algebras.

Theorem 3.8. *Let $I \subseteq A$ be a left ideal, and let $G \subseteq A$. For any left normal form $\mathrm{N}(\bullet; G)$ with respect to G, the following are equivalent.*

- *G is a left Gröbner basis of I.*
- *$\mathrm{N}(f; G) = 0$ for all $f \in I$.*
- *Every $f \in I$ has a standard representation with respect to G.*
- *$\mathrm{N}(S(f, g); G) = 0$ for all $f, g \in G$.*

◁

Proof. See [Lev05a, Theorem 1.16]. □

With this, we also have a version of Buchberger's procedure. Since G-algebras are Noetherian, just like in commutative polynomial rings, this procedure always terminates.

Let us see this in SINGULAR, where `std()` is implemented in the "plural" module for the computation of left Gröbner bases in G-algebras.

Algorithm 5

Input: $G \subseteq A$ finite
Output: A left Gröbner basis $G' \subseteq A$ of ${}_A(G)$

```
1: G' ← G
2: FINISH ← False

3: while FINISH = False do
4:     FINISH ← True
5:     for g, h ∈ G' do
6:         if N(S(g, h); G') ≠ 0 then
7:             G' ← G' ∪ {S(g, h)}
8:             FINISH ← False
9: return G'
```

Example 3.9. Let us again work in the setting of $\mathrm{U}(\mathfrak{sl}_2)$.

```
> LIB "freegb.lib";
> ring r = 0,(e,f,h),Dp;
> setring r;
> matrix D[3][3];
> D[1,2]=-h; D[1,3]=2e; D[2,3]=-2f;
> def A = nc_algebra(1,D);
> setring A;
```

To compute Gröbner bases, we proceed analogously to how we computed Gröbner bases with letterplace rings in Singular.

```
> ideal I = f*e*e*h + 2e*f*f*e, h*f+ 2h*h*e;
> I;

I[1]=2e2f2+e2fh-4efh-2eh2+4ef-2eh
I[2]=2eh2+8eh+fh+8e-2f

> std(I);

_[1]=e
_[2]=h2-2h
_[3]=127fh+8e-254f
```

Note that an expression like `h2` refers to h^2.

```
> ideal J = ef + h + f, h3+f, e2f;
> J;

J[1]=ef+f+h
J[2]=h3+f
J[3]=e2f
```

```
> std(J);

_[1]=h
_[2]=1105f-3948h
```

◁

A. Appendix

A.1. Multiplicative bases and semigroups with zero element

Definition A.1 (semigroup with zero element)**.** Let S be a semigroup. We call an element $d \in S$ a **zero element** or an **absorbing element** if for all $s \in S$ we have $ds = sd = d$, and we call S a **semigroup with zero element**. ◁

Remark A.2. A zero element in a semigroup is unique. ◁

Example A.3. For any ring R, the underlying semigroup with the multiplication in R as the semigroup operation is a semigroup with zero element. Specifically, neutral element of the underlying abelian group, 0, is the zero element.

In particular $(\mathbb{Z}, \cdot)$ is a semigroup with zero element $0 \in \mathbb{Z}$. ◁

Proposition A.4. *If I is a compatible ideal, then A/I has multiplicative basis $\overline{\mathcal{B}} \setminus \{0\}$.* ◁

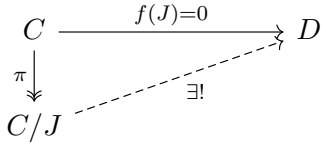
Proof (sketch). We clearly have that $\overline{\mathcal{B}} \setminus \{0\}$ generates A/I as $\mathcal{B}$ generates A, and we now want to show that $\overline{\mathcal{B}} \setminus \{0\}$ is linearly independet in A/I. Let us outline the proof, leaving out a few categorical details.

- To a semigroup S with zero element d, we can assign a (not necessarily unital) associative k-algebra $k(S)$, which is defined as the associative k-algebra with basis elements S, modulo the ideal (d), so that d corresponds to $0 \in kS$. This assignment is a functor from the category of semigroups with zero element to the category of associative unital k-algebras. The k-algebra $k(S)$ then has multiplicative basis $S \setminus \{0\}$.

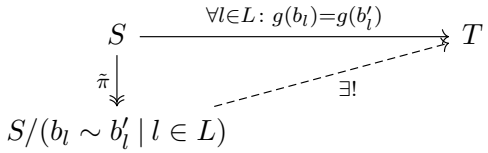
  $$k(\bullet)\colon \mathrm{SemGrp}_0 \to k\text{−Alg}\ ,\ S \mapsto k(S)$$

  This functor is left adjoint to the forgetful functor $k\text{−Alg} \to \mathrm{SemGrp}_0$.

- For $C \in k\text{−Alg}$ and $J \subseteq C$ an ideal, there exists a quotient $\pi\colon C \twoheadrightarrow C/J$, charectarized by following universal property. *We have $\pi(J) = 0$, and any morphism $f\colon C \to D$ with $f(J) = 0$ factorizes uniquely through π.*



- For $S \in \mathrm{SemGrp}_0$, and a collection of elements $b_l, b_l' \in S$ for $l \in L$, there exists a quotient $\tilde{\pi}\colon S \twoheadrightarrow S/ideal{b_l \sim b_l' l \in L}$, characterized by the following universal property. *We have $\tilde{\pi}(b_l) = \tilde{\pi}(b_l')$ for all $l \in L$, and any morphism $g\colon S \to T$ with $g(b_l) = g(b_l')$ for all $l \in L$ factorizes uniquely through $\tilde{\pi}$.*



- **Claim:** *For $S \in \mathrm{SemGrp}_0$ and a collection of elements $b_l, b_l' \in S$ for $l \in L$, we have $k(S/(b_l \sim b_l' \mid l \in L)) \cong k(S)/(b_l - b_l' \mid l \in L)$.*

  Let $D \in k{-}\mathrm{Alg}$. We then have via our adjunction and our universal properties the following isometries of sets, natural in D.

$$\begin{aligned}
&\mathrm{Hom}_{k-\mathrm{Alg}}(k(S/(b_l \sim b_l' \mid l \in L)), D)\\
\cong &\mathrm{Hom}_{\mathrm{SemGrp}_0}(S/(b_l \sim b_l' \mid l \in L), D)\\
\cong &\{g \in \mathrm{Hom}_{\mathrm{SemGrp}_0}(S, D) \mid \forall l \in L\colon g(b_l) = g(b_l')\}\\
\cong &\{f \in \mathrm{Hom}_{k-\mathrm{Alg}}(k(S), D) \mid \forall l \in L\colon f(b_l) = f(b_l')\}\\
\cong &\{f \in \mathrm{Hom}_{k-\mathrm{Alg}}(k(S), D) \mid \forall l \in L\colon f(b_l - b_l') = 0\}\\
\cong &\mathrm{Hom}_{k-\mathrm{Alg}}(k(S)/(b_l - b_l' \mid l \in L), D)
\end{aligned}$$

  By the Yoneda Lemma, we conclude the claim.

- Let $D \in k{-}\mathrm{Alg}$, and let $S \subseteq D$ be a subset that is a semigroup with zero element 0 with the multiplicative structure of D. We then notice that $S\backslash\{0\}$ is a multiplicative basis of D if and only if $k(S) \to D$ (obtained from $S \to D$ via our adjunction) is an isomorphism.

- For our given multiplicative basis $\mathcal{B} \subseteq A$, we notice that $\mathcal{B}_0 = \mathcal{B} \cup \{0\}$ is a semigroup with zero element 0. Furthermore, $\overline{\mathcal{B}_0} \subseteq A/I$ is a semigroup with zero element $\overline{0}$ that generates A/I.

- As I is a compatible ideal, there is a collection of elements $a_m, a_m' \in \mathcal{B}_0$ for $m \in M$ such that $I = (a_m - a_m' \mid m \in M)$. We then have an isomorphism of semigroups with zero element $\mathcal{B}_0/(a_m \sim a_m' \mid m \in M) \cong \overline{\mathcal{B}_0}$.

- We have $A \cong k(\mathcal{B}_0)$.

- We conclude

$$\begin{aligned}
A/I &\cong k(\mathcal{B}_0)/I\\
&\cong k(\mathcal{B}_0)/(a_m - a_m' \mid m \in M)\\
&\cong k(\mathcal{B}_0/(a_m \sim a_m' \mid m \in M))\\
&\cong k(\overline{\mathcal{B}_0})\ .
\end{aligned}$$

Therefore $\overline{\mathcal{B}_0}$ is a multiplicative basis of A/I.

□

A.2. Path algebras

We here present a definition of path algebras different from the one in Definition 1.8. It is here more quickly apparent what the multiplicative basis looks like, and how the grading arises. (See also [DWZ08, Definition 2.1])

Definition A.5. Let M be a nonempty set. We denote by $k^{(M)}$ the set of all functions $f\colon M \to k$ with finite support, meaning $\#\{m \in M \mid f(m) \neq 0\} \in \mathbb{N}_0$. We equip this with a commutative associative k-algebra structure by defining the additive structure by pointwise addition and the multiplicative structure by pointwise multiplication. The constant zero map is then the additive neutral element. ◁

Lemma A.6. For a nonempty set M, the commutative associative k-algebra $k^{(M)}$ is unital if and only if M is finite. ◁

Proof. Let M be finite. Then $k^{(M)} = k^M$ because all maps have finite support for finite M. In particular, we have $\mathbb{1}_M \in k^{(M)}$, the map with constant value 1, which then is the desired unit.

For the converse case, we see that the unit must have value 1 everywhere on M, and for this map to be in $k^{(M)}$, the set M must be finite. □

Definition A.7 (quiver, path algebra)**.** A (finite) **quiver** $Q = (Q_0, Q_1, s, t)$ consists of the following data.

- A nonempty set Q_0, the **vertices**,
- a nonempty set Q_1, the **arrows**,
- a map $s\colon Q_1 \to Q_0$, the **source**, and
- a map $t\colon Q_1 \to Q_0$, the **target**.

For this data, we shall furthermore define the commutative k-algebras $R = k^{(Q_0)}$ and $A = k^{(Q_1)}$ as defined in Definition A.5. Furthermore A is an R-bimodule via the action of the pullbacks $r.a.r' = t^*(r) \cdot a \cdot s^*(r') = (r \circ r) \cdot a \cdot (r' \circ s)$ for $r, r' \in R$ and $a \in A$. We now define the **path algebra** of $Q = (Q_0, Q_1, s, t)$ as the graded tensor algebra of A over R, so

$$kQ := T_R(A)\ ,\ \text{with homogeneous decomposition } kQ = \bigoplus_{d \geq 0} (kQ)_d\ ,\ \text{where}$$

$$(kQ)_d = T_R(A)_d = A^{\otimes_R d}\ .$$

This is also a graded algebra over k with the same grading, with the important detail that the grade 0 component is in general not equal to k. As the multiplication is the

tensor product, we write "$\cdot$" or simply nothing instead of "$\otimes_R$" for the multiplication. This algebra is generated as an R-algebra by the elements of degree 1, and as a k-algebra by the elements of degree 0 and 1. As is usual with tensor algebras, for a k-basis B_1 of $A = (kQ)_1$, the algebra is generated as an R-algebra by B_1, and if B_0 is a k-basis for $R = (kQ)_0$, then kQ is generated as a k-algebra by $B_0 \cup B_1$. The canonical choice of bases here is $B_0 = \{\mathbb{1}_v \mid v \in Q_0\} \subseteq R$ and $B_1 = \{\mathbb{1}_a \mid a \in Q_1\} \subseteq A$, and we identify $Q_0 = B_0$ and $Q_1 = B_1$.

We denote by $Q_{\geq 0}$ the set of all nonzero products of elements in B_0 and B_1, and call such elements **paths**. We furthermore define $Q_d := Q_{\geq 0} \cap (kQ)_d$, where d is called the **length** of a path $v \in Q_d$.[1] For $d = 0$ and $d = 1$, this is consistent with our identification $Q_0 = B_0$ and $Q_1 = B_1$. This means that we write $\mathbb{1}_v = v$ for $v \in Q_0$ and $\mathbb{1}_a = a$ for $a \in Q_1$. A path of length 0, say the path $\mathbb{1}_v = v$ where $v \in Q_0$, is called the **empty** path at v. ◁

Remark A.8.

- kQ is a unital algebra if and only if Q_0 is finite, since then $R = k^{(Q_0)} = k^{Q_0}$ is unital with unit $1_R = \mathbb{1}_{Q_0} \in R$ by Lemma A.6, and we then have $1_{kQ} = 1_R \in R \subseteq kQ$.

- We have $\operatorname{span}_k Q_d = (kQ)_d$.

- Let $v, w \in Q_0$ and $a, b \in Q_1$. Note that we have $ab \neq 0$ if and only if $t(a) = s(b)$ and also note that $va = a$ if and only if $s(a) = v$ and $av = a$ if and only if $t(a) = v$, resulting in zero otherwise, and finally observe that $vw = \delta_{v,w}$. We arrive at the fact that we can uniquely write any element $x \in Q_{\geq 0}$ as

$$x = v_0 a_1 v_1 a_2 v_2 \dots v_{d-1} a_d v_d \ ,$$

  where $v_i \in Q_0$ and $a_i \in Q_1$ such that $s(a_i) = v_{i-1}$ and $t(a_i) = v_i$, where indeed d is the length of x. This is in line with a different definition of the path algebra, where paths are defined as words of such form and where the multiplication is defined by specific concatenation rules.

- We can extend the source and target functions s and t to all of $Q_{\geq 0}$, in fact to nonzero scalar multiples of such elements, by defining $s(y) = v_0$ and $t(y) = v_d$ for $y = \lambda \cdot x$ with $\lambda \in k^\times$ and $x = v_0 a_1 v_1 a_2 v_2 \dots v_{d-1} a_r v_d \in Q_{\geq 0}$ presented as above. We call $s(y)$ the **source** of y and $t(y)$ the **target** of y. With this, we have for y and z of this form that $y \cdot z \neq 0$ if and only if $t(y) = s(z)$.

- It is also common to write $\mathbb{1}_v = 1_v$ for $v \in Q_0$, which is also used in context of the fact that these are idempotents. For $v, w \in Q_0$ we have that $kQ_{v,w} := 1_v \cdot kQ \cdot 1_w = \operatorname{span}_k(Q_{v,w})$, where $Q_{v,w}$ is the set of all paths that have source v and target w. For $u, v, w, x \in Q_0$ we notice $\operatorname{span}_k(kQ_{u,v} \cdot kQ_{w,x}) = \delta_{v,w} \cdot kQ_{u,x}$, and also see that $kQ = \bigoplus_{v,w \in Q_0} kQ_{v,w}$.

◁

[1] Analogously we define $Q_{\geq d} = Q_{\geq 0} \cap (kQ)_{\geq d}$.

Bibliography

[Coh08] Arjeh M. Cohen. "Non-commutative polynomial computations". In: (July 2008). URL: https://www.researchgate.net/publication/228565357_Non-commutative_polynomial_computations.

[Dec+21] Wolfram Decker et al. **Singular 4-2-1 — A computer algebra system for polynomial computations**. http://www.singular.uni-kl.de. 2021.

[DWZ08] Harm Derksen, Jerzy Weyman, and Andrei Zelevinsky. "Quivers with Potentials and their Representations I: Mutations". In: (2008). URL: https://arxiv.org/abs/0704.0649v4.

[GMU98] Ed Green, Teo Mora, and Victor Ufnarovski. "The Non-Commutative Grabner Freaks". In: **Symbolic Rewriting Techniques**. 1st ed. Progress in Computer Science and Applied Logic 15. Birkhäuser Basel, 1998, pp. 93–104. ISBN: 978-3-0348-9779-2,978-3-0348-8800-4.

[Gre99] Edward L. Green. "Noncommutative Gröbner Bases, and Projective Resolutions". In: Progress in Mathematics 173. Basel, Switzerland: Birkhäuser Verlag, 1999, pp. 29–60.

[Lev05a] Viktor Levandovskyy. "Non–commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementation". Universität Kaiserslautern, 2005.

[Lev05b] Viktor Levandovskyy. "PBW Bases, Non–Degeneracy Conditions and Applications". In: **Proceedings of the ICRA X conference. Volume 45., AMS. Fields Institute Communications**. 2005, pp. 229–246.

[LL09] Roberto La Scala and Viktor Levandovskyy. "Letterplace ideals and noncommutative Gröbner bases". In: **Journal of Symbolic Computation** 44 (2009), pp. 1374–1393.

[Mor94] Teo Mora. "An introduction to commutative and noncommutative Gröbner bases". In: Theoretical Computer Science 134 (1994), pp. 131–173. ISSN: 0304-3975.

[Xiu12] Xinqiang Xiu. "Non-Commutative Gröbner Bases and Applications". Universitiät Passau, 2012.

[Zei19] Karim Josef Abou Zeid. "Letterplace Gröbner Bases, their Implementation and Applications". RWTH Aachen, 2019.