On Gröbner bases

and some applications to symmetric functions and free resolutions

Bachelor's thesis in Mathematics

Axel Sarlin
axelhu@kth.se

Innokentij Zotov
zotov@kth.se

Advisor:
Tilman Bauer

Examiner:
Mårten Olsson

Royal Institute of Technology
Stockholm, 2015

Abstract

First introduced by Bruno Buchberger in 1965, Gröbner bases have now become a standard tool in computational algebra. Gröbner bases are used in a diverse spectrum of applications, ranging from tasks such as solving systems of equations, to applications where their properties are used as a stepping stone for further abstract algorithms.

In this paper we collect some now classical results and some recent developments in a way that may be used as an introduction to this rich subject for readers with some background in basic algebra. We provide examples of the classical methods of equation solving and examples of using Gröbner theory to calculate other interesting algebraic objects.

Notation and symbols

symbol	**meaning**
$\square$	end of proof
$\triangle$	end of example
$\mathbb{N}$	$\{0, 1, 2, \ldots\}$
$\trianglelefteq$	ideal in
$(f_1, \ldots, f_s)$	ideal generated by $\{f_1, \ldots, f_s\}$
$\langle \mathbf{f}_1, \ldots, \mathbf{f}_s \rangle$	submodule generated by $\{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$
A	the polynomial ring in n variables over a field k
A^n	the free module $A \times \cdots \times A$ of dimension n
$\mathbb{T}^n$	the set of power products in A
$<$	lesser than, term order
$f \xrightarrow{g} h$	polynomial reduction of f to h by g
$f \xrightarrow{G}_{+} h$	polynomial reduction of f to h by G in multiple steps
$\leq$	lesser than or equal to, submodule of
$\prec$	induced term order
$\cong$	isomorphic to
im	image
ker	kernel
$\oplus$	direct sum
$\otimes$	tensor product
$\mathrm{Hom}(M, N)$	the set of A-module homomorphisms from M to N
$\mathrm{Ext}^n(M, N)$	the extension group at position n between M and N

Contents

1. Introduction

Since its inception, the meaning of the word *algebra* has shifted somewhat. Originally refering to the art of solving equations, the term now encompasses a more general notion - modern algebra is the study of general worlds and objects that we can formulate equations in. The concepts of numbers and equations have been generalized by definitions such as rings, polynomials and vector spaces. For a more lucid and complete account of the development of algebra, we refer to the first chapter of [Pin10], aptly titled “Why abstract algebra?”.

The aim of this paper is to present the foundations of Gröbner bases, a computational tool for solving systems of equations, in the setting of a polynomial ring over a field.

We begin section 2.1 by recalling some elementary concepts from abstract algebra, and in 2.2 we proceed by presenting some further concepts from commutative algebra that are necessary. Concluding the first section, we discuss some implications from the area of algebraic geometry in 2.3.

The third section covers the fundamentals of Gröbner theory. In 3.1 we introduce some technical definitions needed for the definition of Gröbner bases in 3.2. We then proceed by presenting a constructive algorithm for finding Gröbner bases known as Buchbergers algorithm in 3.3. In 3.4 and 3.5 we discuss some further properties and show examples of Gröbner bases, including a construction of a Gröbner basis for the elementary symmetric polynomials.

In the next section we cover the basic theory of modules and a natural generalization of Gröbner bases to modules over a polynomial ring in 4.1 and 4.2. In 4.3 we discuss *syzygies* as a way to describe linear dependence of a set of generators. In 4.4 we briefly cover free resolutions and how syzygies can be used to show classical results regarding them. In the concluding sections 4.4 to 4.7 we present methods for explicit calculations of algebraic objects such as Hom and Ext.

2. Preliminaries

2.1. Some basic algebraic concepts, definitions and examples

We will, for most parts, assume some familiarity with basic concepts of mathematics, but for clarity and completeness we will include some basic definitions and examples. The definitions of 2.1 will be familiar to any student of an introductury course in algebra. Further concepts that may be new to such a reader will be presented in 2.2. For a more exhaustive account of these objects, we recommend the book *Abstract Algebra* by Dummit and Foote, [DF04].

Definition 2.1. A GROUP is a set G with a binary operation $\star$ defined on its elements, that satisfy the following:

- *Closure:* for all $a, b \in G$, $a \star b \in G$.
- *Associativity:* for all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.
- *Identity element:* there exists an element $e \in G$ such that $a \star e = e \star a = a$ for all $a \in G$.
- *Inverse:* for all $a \in G$, exists an element a^{-1} such that $a \star a^{-1} = a^{-1} \star a = e$.

Remark. One often writes the group as $(G, \star)$ to emphasize the operation in question. If the context makes it obvious, the operation is often omitted and written as $a \star b = ab$.

Examples 2.2. The set of integers $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ is a group with the operation of addition. Similarly the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are groups under addition. The natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ with $+$ do not however form a group since it lacks inverse elements. $\mathbb{Z}[x]$, the polynomials with integer coefficients in one indeterminate x is a group under addition. △

Definition 2.3. A group G is said to be ABELIAN (or commutative) if for any two $a, b \in G$, $ab = ba$.

Definition 2.4. A RING is a set R with two binary operations $+$ and $\star$ defined on its elements, that satisfy the following:

- $(R, +)$ is an abelian group.
- *Closure:* for all $a, b \in R$, $a \star b \in R$.
- *Associativity:* for all $a, b, c \in R$, $(a \star b) \star c = a \star (b \star c)$.
- *Identity element:* there exists an element $1 \in R$ such that $a \star e = e \star a = a$ for all $a \in R$.
- *Distributivity:* for all $a, b, c \in R$, $a \star (b + c) = a \star b + a \star c$ and $(a + b) \star c = a \star c + b \star c$.

Remark. The second operation above is often refered to as multiplication and written with $a \cdot b$ or ab. The existence of a multiplicative identity element is often referred to as *unitality.* Some authors choose not to include this in the base definition of a ring.

Examples 2.5. The set of integers $\mathbb{Z} = \{0, 1, -1, 2, -2...\}$ is a ring with the operations being addition and multiplication. The same holds for $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

$\mathbb{Z}[x]$, the set of polynomials with integer coefficients in one variable, is a ring. The same holds for polynomials in two or any number n variables, $\mathbb{Z}[x, y]$ resp. $\mathbb{Z}[x_1, ..., x_n]$. △

Definition 2.6. A ring R is said to be COMMUTATIVE if the multiplication is commutative, i.e. for any two $a, b \in R$, $ab = ba$.

We now make precise the construction $\mathbb{Z}[x]$ in the example above.

Definition 2.7. For a commutative ring R, the POLYNOMIAL RING $R[x]$ is the set of finite sums of the form $p(x) = p_0 + p_1x + \ldots + p_nx^n$ for some natural number n, coefficients $p_0, \ldots, p_n \in R$ and the indeterminate variable x. A summand in this sum is called a TERM.

We define addition and multiplication as for the usual polynomials in a determinate x in basic algebra. Let $q(x) = q_0 + q_1x + \ldots + q_mx^m$ and, without loss of generality, $n \geq m$. We say $q_i = 0$ for $i > m$ and define

$$p(x) + q(x) = (p_0 + q_0) + (p_1 + q_1)x + \ldots + (p_n + q_n)x^n, \qquad p(x)q(x) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} p_j q_{i-j} \right) x^i.$$

The ring of multivariate polynomials over R is defined in the same manner and is constructed as

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x].$$

Definition 2.8. A (two-sided) IDEAL is a subset I of a ring R such that

- *Closure:* I is a ring.
- *Absorption:* for all $r \in R$ and $i \in I$, $ri \in I$ and $ir \in I$.

The statement that I is an ideal of R is often written $I \trianglelefteq R$. The set of ring elements that can be written on the form $r_1a_1 + \ldots + r_sa_s$ for a fixed set $\{a_1, \ldots, a_s\} \subseteq R$ and ring elements $r_i \in R$ is an ideal of R. This is said to be the ideal GENERATED BY $\{a_1, \ldots, a_s\}$ and is written as $(a_1, \ldots, a_s)$.

Examples 2.9. The set of even integers $2\mathbb{Z} = \{0, 2, -2, 4, -4, ...\}$ is an ideal of $\mathbb{Z}$. Similarly, $n\mathbb{Z}$ is an ideal for any integer n.

The set of polynomials $p \in \mathbb{Z}[x]$ that can be written $p = (1 + x)q$ for some $q \in \mathbb{Z}[x]$ is an ideal, written $(1 + x) \trianglelefteq \mathbb{Z}[x]$. △

Remark. When used in proofs in this text, we will show that a subset I is an ideal of R by first showing closure under subtraction (taking additive inverses), that is, given $x, y \in I$ the difference $x - y$ is also in I. Closure under multiplication by elements of R will then yield both conditions in the definition above.

Definition 2.10. The QUOTIENT RING R/I of an ideal I in a ring R is defined by

$$R/I = \{r + I \mid r \in R\}$$

with well-defined addition and multiplication by $(a+I)+(b+I) = (a+b)+I$ and $(a+I)(b+I) = ab + I$.

Examples 2.11. For the ring $\mathbb{Z}$ and the ideal $3\mathbb{Z}$, the quotient ring is $\mathbb{Z}/3\mathbb{Z} = \{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\} = \{0, 1, 2\}$, informally the integers modulo 3. Some illustrative valid statements for this ring include $1 + 2 = 0$, $2 \cdot 2 = 1$ and $1 = -2$.

In the quotient ring $\mathbb{R}[x]/(x^2+1)$, we have that $x^2+1+(x^2+1) = 0+(x^2+1)$ and $x^2+(x^2+1) = x^2 + 1 - 1 + (x^2 + 1) = -1 + (x^2 + 1)$. Informally, in this quotient ring, $x^2 + 1$ is "killed", or, equivalently, occurrences of x^2 are replaced by -1. △

Definition 2.12. A FIELD is a set k such that

- k is a commutative ring.
- *Multiplicative inverse:* for all non-zero $r \in k$ there is a $r^{-1} \in k$ such that $r^{-1}r = 1$.

Examples 2.13. The set of rational numbers $\mathbb{Q}$ as well as the real numbers $\mathbb{R}$ are fields. The quotient ring $\mathbb{Z}/3\mathbb{Z}$ is a field, as any non-zero element has a multiplicative inverse: $1 \cdot 1 = 1$, $2 \cdot 2 = 1$. Indeed, the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field for any prime number p, such as $p = 57$. △

Remark. In a field k, any element y can be reached from some given element x through multiplication by yx^{-1}. From this observation we easily see that if I is an ideal of k, either $I = (0) = \{0\}$ or $I = (1) = k$. Furthermore, if $xy = 0$ for some $x, y \in k$, then either $x = 0$ or $y = 0$. That is, every field is an *integral domain.*

We now define the concept of a structure preserving map between rings, essential in the study of these objects. These are functions from the underlying set of a ring to that of another ring that respect the operations of both rings.

Definition 2.14. A HOMOMORPHISM (of rings) is a function $f : R \to S$ between two rings R, S such that:

- *Multiplicativity:* for all $a, b \in R$, $f(ab) = f(a)f(b)$.
- *Additivity:* for all $a, b \in R$, $f(a + b) = f(a) + f(b)$.
- the multiplicative identity 1_R of R is mapped to the multiplicative identity 1_S in S.

A ring homomorphism that is bijective is an ISOMORPHISM. If an isomorphism between R and S exists, we say that R is ISOMORPHIC to S and write $R \cong S$.

Examples 2.15. For the ring $\mathbb{Z}$, the map $f(n) = 2n$ defines a homomorphism $f : \mathbb{Z} \to \mathbb{Z}$. This can also be used, for instance, to define a homomorphism $f : \mathbb{Z} \to \mathbb{Q}$.

The map between the quotient ring $\mathbb{R}[x]/(x^2 + 1)$ and the complex numbers $\mathbb{C}$ defined by mapping x to the imaginary unit i, or more explicitly $a + bx \mapsto a + bi$ is an isomorphism. Hence

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

△

2.2. Further definitions and some useful results

From the fundamental concepts presented in 2.1 we may now introduce some additional definitions necessary for the machinery of Gröbner theory. First we present some key concepts of commutative algebra and then we turn our attention towards the central objects of algebraic geometry in 2.3.

Firstly we define a property of a ring that will be essential for our foray into computational algebra.

Definition 2.16. A ring R is said to be NOETHERIAN if for every ascending chain of ideals $I_i \trianglelefteq R$

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

there exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = I_{N+2} = \cdots$. That is, R is Noetherian if and only if there are no infinite strictly ascending chains of ideals.

This property can be formulated in more tangible terms for commutative rings as follows:

Theorem 2.17. A commutative ring R is Noetherian if and only if every ideal $I \trianglelefteq R$ is finitely generated, i.e. any such I has a finite generating set.

Proof. Assume that R is Noetherian and that there exists an $I \trianglelefteq R$ that does not have a finite generating set. Let $f_1 \in I$. Then there exists $f_2 \in I$ such that $f_2 \notin (f_1)$ so that $(f_1) \subsetneq (f_1, f_2)$. Continuing in this fashion we obtain a strictly ascending chain of ideals, which contradicts the Noetherianity of R.

Conversely, assume that every ideal of R is finitely generated. Consider an ascending chain of ideals of R

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots .$$

Construct $I = \bigcup_k I_k$ and let $x, y \in I$. Then $x \in I_i$ and $y \in I_j$ for some i, j. Without loss of generality we are free to take $i \leq j$ so that $I_i \subseteq I_j$ and $x, y \in I_j$, which is an ideal in R and thus closed under subtraction. From the definition it is clear that I absorbs elements of R. Hence $I \trianglelefteq R$.

Thus I is finitely generated, $I = (f_1, \ldots, f_s)$. Then for every $i \in \{1, \ldots, s\}$ there exists N_i such that $f_i \in I_{N_i}$. Take now $N = \max(N_1, \ldots, N_s)$. Then $f_i \in I_N$ for $i \in \{1, \ldots, s\}$ so that $I \subseteq I_N$, i.e. $I = I_N$. Hence $I_N = I_{N+1} = I_{N+2} = \cdots$ and the ascending chain terminates. □

Examples 2.18. A field k is Noetherian since, as we saw above; if $I \trianglelefteq k$, then either $I = (0) = \{0\}$ or $I = (1) = k$.

The polynomial ring (in finitely many variables) $k[x_1, ..., x_n]$ is Noetherian, which we shall see as a consequence of Theorem 2.20.

A non-Noetherian ring may be realized by, for instance, taking a polynomial ring in infinitely many variables. △

The theorem we shall state below is indispensable in the theory of Gröbner bases in that it, as we shall see in further sections, guarantees that investigated ideals have a finite set of generators which in turn guarantees that our algorithmic operations terminate after a finite number of steps. First it is necessary to define some concepts in a polynomial ring.

Definition 2.19. Let R be a commutative ring and $p(x) = p_0 + p_1 x + \ldots + p_n x^n \in R[x]$. We define $\mathrm{LT}(p)$, the LEADING TERM of p to be the term of the form cx^i for some non-zero $c \in R$ and maximal i, that is, $\mathrm{LT}(p) = p_n x^n$. c is said to be the LEADING COEFFICIENT of p, $c = \mathrm{LC}(p)$. Furthermore we define $\deg(p) \in \mathbb{N}$ to be the DEGREE of a polynomial, the highest occurring power of x so that $\deg(p) = n$.

Remark. If R is a commutative ring that is an integral domain (that is, given $xy = 0$, either $x = 0$ or $y = 0$), then $\deg(pq) = \deg(p) + \deg(q)$ for non-zero $p, q \in R[x]$.

Theorem 2.20. (*Hilbert basis theorem*) If the commutative ring R is Noetherian, then $R[x]$ is Noetherian.

Proof. Let $J \trianglelefteq R[x]$. We will constructively show that J is finitely generated. Define

$$I_n = \{r \in R \,|\, \text{there exists a } p \in J \text{ such that } \deg(p) = n \text{ and } r = \mathrm{LC}(p)\} \cup \{0\}.$$

Then for $p, q \in J$ corresponding to some $r, s \in I_n$, respectively, as in the definition of I_n, $\deg(p-q) = n$ if $r \neq s$ so that $\mathrm{LC}(p - q) = r - s$ and $r - s \in I_n$ (if $r = s$, then $r - s = 0 \in I_n$), so that I_n is closed under subtraction. Given some $t \in R$ obviously $\deg(tp) = n$ and $\mathrm{LC}(tp) = tr$ so that I_n absorbs elements of R. Hence $I_n \trianglelefteq R$.

Furthermore, for a $p \in J$ corresponding to some $r \in I_n$, we have that $\deg(xp) = n + 1$ and $\mathrm{LC}(xp) = r$ so that $r \in I_{n+1}$. Hence $I_n \subseteq I_{n+1}$ and we have an ascending chain of ideals of R. Since R is Noetherian, there exists $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$ and every ideal in the chain is finitely generated, $I_i = (r_{i1}, \dots, r_{it_i})$.

Let now $f_{ij} \in J$ be the polynomial corresponding to r_{ij} as in the definition of I_i (i.e. of degree i and such that $\mathrm{LC}(f_{ij}) = r_{ij}$) for each $i \in \{1, \dots, N\}$ and $j \in \{1, \dots, t_i\}$. Construct $J' = (f_{ij} \mid i \in \{1, \dots, N\}, j \in \{1, \dots, t_i\}) \subseteq J$ and let $f \in J$ with $\deg(f) = n$. We shall show that $f \in J'$ by induction over n.

For the base step, if $f = 0$ or $n = 0$, then $f \in I_0$ and hence $f \in J'$. For $n > 0$, assume that the elements of J of degree $< n$ are in J' and let $r = \mathrm{LC}(f)$. We have the following cases:

If $n \leq N$, then the leading coefficient of f is in I_n and r can be written as $r = \sum_j s_j r_{nj}$ for s_j in R. Then for $g = \sum_j s_j f_{nj} \in J'$, we have $\deg(g) = n$ and $\mathrm{LC}(g) = r$. We thus have $\deg(f - g) < n$ and, since $f - g \in J$, by induction, $f - g \in J'$ so that $f \in J'$.

If $n > N$, then $f \in I_n = I_N$ so that $r = \sum_j s_j r_{Nj}$ for $s_j \in R$. Construct $g = \sum_j s_j x^{n-N} f_{Nj} \in J'$. Evidently, $\deg(g) = n - N + N = n$ and $\mathrm{LC}(g) = r$ so that $\deg(f - g) < n$. By induction, $f - g \in J'$ and thus $f \in J'$. Hence $J = J'$ and is finitely generated. □

Corollary 2.21. The multivariate polynomial ring $k[x_1, \dots, x_n]$ over a field k is Noetherian.

Proof. This follows from an easy induction over n using the Noetherianity of k and the fact that

$$k[x_1, \dots, x_n] = k[x_1, \dots, x_{n-1}][x].$$

□

2.3. Algebraic geometry and solution sets

The idea of representing the solutions of equations geometrically is common and essential in almost any application of mathematics. This idea is formalized properly by the concept of solution sets, varieties, that exhibit geometrical properties of algebraic objects as well as radical of ideals exhibiting algebraic properties of geometrical objects. The famous zero locus theorem of Hilbert, the *Nullstellensatz*, captures this connection in a beautiful way. To understand the utility that the essentially purely algebraic construction of Gröbner bases carries for geometrical purposes, we now briefly introduce some of these concepts.

Definition 2.22. For a(n algebraically closed) field k and a set of polynomials $F = \{f_1, ...\} \subseteq k[x_1, ..., x_n]$, we define the VARIETY of F by

$$\mathcal{Z}(F) = \{\, p \in k^n \mid f(p) = 0 \ \forall f \in F\}.$$

Definition 2.23. For a subset V of k^n, we define the VANISHING IDEAL of V by

$$\mathcal{I}(V) = \{\, f \in k[x_1, ..., x_n] \mid f(p) = 0 \ \forall p \in V\}.$$

Definition 2.24. For any ideal I in a ring R, we define the RADICAL of the ideal by

$$\sqrt{I} = \{\, r \in R \mid \exists n \in \mathbb{N} : \ r^n \in I\}.$$

Theorem 2.25. (*Hilbert Nullstellensatz*) For an algebraically closed field k and any proper ideal I of $k[x_1, ..., x_n]$, the following is true:

$$\sqrt{I} = \mathcal{I}(\mathcal{Z}(I)).$$

This well-known result was first shown (as one might guess) by Hilbert in 1890. Proofs of this theorem can be found in any proper treatment on commutative algebra or algebraic geometry, for instance in Atiyah's and Macdonald's *Introduction to Commutative Algebra*, [AM69]. We will not make explicit use of this theorem, but include it because of its significance and as an indication of how methods on ideals (such as Gröbner bases) can be related to other areas of mathematics.

Example 2.26. For the ideal $I = (x^3)$ in $\mathbb{C}[x]$, polynomials in the algebraically closed field $\mathbb{C}$, we have a very trivial variety $\mathcal{Z}(I) = \{0\}$. The vanishing ideal of this variety is the ideal of polynomials that vanish on 0. This is any polynomial without a constant term, meaning that $\mathcal{I}(\mathcal{Z}(I)) = (x)$, which is exactly the radical of $I = (x^3)$. △

Example 2.27. In the two-dimensional real plane a circle can be defined by the solutions to the equation $x^2 + y^2 = 1$. An ellipse can similarly be described by the equation $x^2/3 + 3y^2 = 1$. The circle and the ellipse intersect each other at

$$\left(\pm\sqrt{3}/2,\ \pm 1/2\right) \in \mathbb{R}^2.$$

However, $\mathbb{R}$ is not algebraically closed, so we consider these objects as subsets of $\mathbb{C}$. The real valued solution points are shown in figure 1.

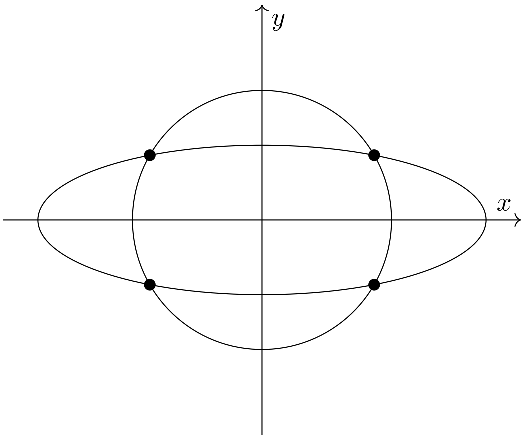

Figure 1: Intersection of circle and ellipse in $\mathbb{R}^2$

For an algebraic treatment we can associate the circle with the ideal $I_1 = (x^2 + y^2 - 1)$ and the ellipse with $I_2 = (x^2/3 + 3y^2 - 1)$ and identify them with the varieties $\mathcal{Z}(I_1)$ and $\mathcal{Z}(I_2)$.

The intersection of two varieties is the variety of the union of the ideals,

$$\mathcal{Z}(I_1) \cap \mathcal{Z}(I_2) = \mathcal{Z}(I_1 \cup I_2)$$

but in general, unions of ideals may not be ideals. However,

$$I_1 \cup I_2 \subseteq I_1 + I_2 = \{a + b \mid a \in I_1, b \in J_2\} = (x^2 + y^2 - 1,\ \frac{1}{3}x^2 + 3y^2 - 1)$$

and therefore $\mathcal{Z}(I_1 \cup I_2) \supseteq \mathcal{Z}(I_1 + I_2)$. Since any element of the intersection $\mathcal{Z}(I_1) \cap \mathcal{Z}(I_2)$ will be in the variety $\mathcal{Z}(I_1 + I_2)$ of the sum, this implies that $\mathcal{Z}(I_1 \cup I_2) = \mathcal{Z}(I_1 + I_2)$.

Thus, the intersection points are described by the variety of the sum of the ideals:

$$\mathcal{Z}(I_1 \cup I_2) = \mathcal{Z}(I_1 + I_2) = \left\{p \in \mathbb{C}^2 \mid f(p) = 0 \quad \forall f \in I_1 + I_2\right\}$$

which gives us the following set of real valued solutions:

$$\left\{\left(\pm\sqrt{3}/2,\ \pm 1/2\right) \in \mathbb{R}^2\right\}.$$

In section 3.4 we will show how to obtain this result by computing a Gröbner basis for the ideal $I_1 + I_2 = (x^2 + y^2 - 1,\ \frac{1}{3}x^2 + 3y^2 - 1)$. △

3. Gröbner basics

Throughout this section, we will for the most part paraphrase the terminology and exposition in [AL94], following the same steps in our proofs unless otherwise indicated. The remarks and examples, however, mostly reflect the thoughts of the writers. The former are mostly things we have picked up from different sources on our way and the latter constitute a mixed collection of exercises and standard examples found in literature (with references) as well as our own examples.

3.1. Term orders, leading terms and division algorithm

The modern body of Gröbner theory consists of a set of computational tools and results that enables explicit calculations of various algebraic objects. The central notion for this framework is that of Noetherianity, which as previously mentioned is the property that guarantees the existence of a finite generating set for an ideal. Gröbner bases are a particular kind of finite generating sets for ideals in (Noetherian) polynomial rings, so this allows us in turn to introduce algorithmic methods for finding these in a finite number of steps. The central aspects of this theoretical framework that enables these constructive methods will be presented in this section.

Here we introduce some important definitions required to define Gröbner bases. Firstly, we recall the concept of division in a polynomial ring $k[x]$ over a field and then see how this definition can be extended to the multivariate case. The following formulation is the *long division* of basic algebra:

Definition 3.1. Given $f, g, h \in k[x]$, we say that f REDUCES TO h BY g or write $f \xrightarrow{g} h$ if and only if $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$ and

$$h = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g.$$

If furthermore f is reduced by g in a number of steps, such as when $f \xrightarrow{g} h \xrightarrow{g} r$, we write $f \xrightarrow{g}_{+} r$.

Theorem 3.2. (*Euclidean property of* $k[x]$) For any $f, g \in k[x]$ such that $g \neq 0$, there exist unique $q, r \in k[x]$ such that $f = qg + r$ with either $r = 0$ or $\deg(r) < \deg(g)$.

Proof. Due to [DF04]. Assume $f \neq 0$ (otherwise, $q = r = 0$) and let $n = \deg(f)$, $m = \deg(g)$. We show existence of q and r by induction over n.

If $n < m$, let $q = 0$ and $r = f$. Assume thus that $n \geq m$ and let $f \xrightarrow{g} f'$ so that

$$f' = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g.$$

Then $\deg(f') < \deg(f)$. By induction, there exist q' and r' such that $f' = q'g + r'$ and either $r' = 0$ or $\deg(r') < \deg(g)$. Defining $r = r'$ and

$$q = q' + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}$$

we can write $f = qg + r$ so that either $r = 0$ or $\deg(r) < \deg(g)$.

Assume now that for f and g we can write $f = q_1 g + r_1$ and $f = q_2 g + r_2$ as above. Then $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$ so that $\deg(r_1 - r_2) = \deg((q_2 - q_1)g) < \deg(g)$. Since $\deg((q_2 - q_1)g) = \deg(q_2 - q_1) + \deg(g)$ if the polynomials are non-zero (as remarked earlier, k is an integral domain), we necessarily have $q_2 - q_1 = 0$ so that $q_1 = q_2$ and, consequently, $r_1 = r_2$ so that the q and r are unique. □

Example 3.3. Let $f = x^3 + 2x^2 + x$ and $g = x + 1$. We identify $\mathrm{LT}(f) = x^3$ and $\mathrm{LT}(g) = x$. The reduction can be done in two steps:

$$\begin{aligned} h_1 = \quad & f \; - \; \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g & = x^3 + 2x^2 + x - \frac{x^3}{x}(x+1) = x^2 + x \\ h_2 = \quad & h_1 - \frac{\mathrm{LT}(h_1)}{\mathrm{LT}(g)} g & = x^2 + x - \frac{x^2}{x}(x+1) = 0, \end{aligned}$$

so that $f \xrightarrow{g}_+ 0$. △

For polynomial division to be applicable in a multivariate ring, we need a way to compare monomials consisting of several indeterminates. This is formulated using the concept of term orders. Henceforth we will denote our multivariate polynomial ring $k[x_1, \ldots, x_n]$ by A.

Definition 3.4. By a MONOMIAL or POWER PRODUCT in A we refer to a product of the form $X = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for some powers $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. A TERM in A is of the form cX with $c \in k$ and a monomial X. We shall denote the set of the power products of A by $\mathbb{T}^n$.

Definition 3.5. A TERM ORDER on $\mathbb{T}^n$ is a total order $<$ on $\mathbb{T}^n$ (that is, given two monomials $X, Y \in \mathbb{T}^n$ exactly one of the following holds: $X < Y$, $X > Y$ or $X = Y$) such that:

- $1 < X$ for all $X \in \mathbb{T}^n$ such that $X \neq 1$.
- If $X < Y$, then $ZX < ZY$ for all $Z \in \mathbb{T}^n$.

Remark. For two terms $P = cX, Q = dY$, we say $P < Q$ if $X < Y$ with respect to the term order $<$ on $\mathbb{T}^n$.

The following result connects the mechanism of multivariate term orders to the usual univariate operations:

Lemma 3.6. Let $<$ be a term order on $\mathbb{T}^n$ and $X, Y \in \mathbb{T}^n$. If X divides Y, then $X \leq Y$.

Proof. Since X divides Y, there exists $Z \in \mathbb{T}^n$ such that $Y = XZ$ and from the term order definition, $Z \geq 1$. Then $Y = XZ \geq X$, again from the definition. □

Recall that for the univariate case, polynomial division returned as output a remainder r of strictly lesser degree than that of g. To assure that reduction can be performed in a finite number of steps we need to verify the nonexistence of infinite strictly descending chains of terms. Any total order $<$ on A that satisfies the two conditions in the definition is then a valid way of comparing power products in A, as is seen from the following consequence of the Hilbert basis theorem in 2.2:

Theorem 3.7. Any term order on $\mathbb{T}^n$ is a well-ordering. That is, for a given term order $<$ on $\mathbb{T}^n$, any collection of power products $T \subseteq \mathbb{T}^n$ has a minimal element $X \in T$ such that for any $Y \in T$, $X \leq Y$.

Proof. Assume to the contrary that there is no such minimal X. Then there exist power products $X_i \in \mathbb{T}^n$ for $i \in \mathbb{N}$ such that

$$X_1 > X_2 > X_3 > \cdots$$

and there exists a collection of ideals of A

$$(X_1) \subseteq (X_1, X_2) \subseteq (X_1, X_2, X_3) \subseteq \cdots .$$

We shall show that equality between two such consecutive ideals cannot hold. Assume that $(X_1, \ldots, X_n) = (X_1, \ldots, X_n, X_{n+1})$. Then we can write

$$X_{n+1} = \sum_{i=1}^{n} p_i X_i$$

for polynomials $p_i \in A$. Every summand is then of the form $p_i X_i$ where X_i divides every term in $p_i X_i$ so that every term on the right-hand side is divisible by an X_i for some $i \in \{1, \ldots, n\}$. Since equality holds, X_{n+1} must appear on the right-hand side and is thus divisible by some X_i. By Lemma 3.6 above we then necessarily have $X_i \leq X_{n+1}$ with $n+1 > i$, which is a contradiction. Hence we obtain the following strictly ascending chain of ideals of A

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots,$$

which contradicts the Noetherianity of A by the Hilbert basis theorem. □

We shall now state some commonly used term orders on $\mathbb{T}^n$. Let $X = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ and $Y = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ for $(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$.

Definition 3.8. The LEXICOGRAPHICAL (lex) term order on $\mathbb{T}^n$, with $x_1 > x_2 > \cdots > x_n$ is defined as

$$X < Y \iff \alpha_i < \beta_i \text{ holds for the first } 1 \leq i \leq n \text{ such that } \alpha_i \neq \beta_i.$$

Example 3.9. Using lex and $x_1 > x_2$,

$$1 < x_2 < x_2^2 < x_1 < x_1 x_2 < x_1 x_2^2 < x_1^2.$$

△

Definition 3.10. The DEGREE LEXICOGRAPHICAL (deglex) term order on $\mathbb{T}^n$ with $x_1 > x_2 > \cdots > x_n$ is defined as

$$X < Y \iff \begin{array}{l} \left(\sum\limits_{i=1}^{n} \alpha_i < \sum\limits_{i=1}^{n} \beta_i\right) \text{ or} \\ \left(\sum\limits_{i=1}^{n} \alpha_i = \sum\limits_{i=1}^{n} \beta_i \text{ and } X < Y \text{ with respect to lex } x_1 > x_2 > \cdots > x_n\right). \end{array}$$

Example 3.11. Using deglex and $x_1 > x_2$,

$$1 < x_2 < x_1 < x_2^2 < x_1 x_2 < x_1^2 < x_2^3 < x_1^3.$$

△

Definition 3.12. The DEGREE REVERSE LEXICOGRAPHICAL (degrevlex) term order on $\mathbb{T}^n$ with $x_1 > x_2 > \cdots > x_n$ is defined as

$$X < Y \iff \begin{array}{l} \left(\sum\limits_{i=1}^{n} \alpha_i < \sum\limits_{i=1}^{n} \beta_i\right) \text{ or} \\ \left(\sum\limits_{i=1}^{n} \alpha_i = \sum\limits_{i=1}^{n} \beta_i \text{ and } \alpha_i > \beta_i \text{ holds for the first } n \geq i \geq 1 \text{ such that } \alpha_i \neq \beta_i\right). \end{array}$$

Example 3.13. Using degrevlex and $x_1 > x_2 > x_3$, we have $x_1^2 x_2 x_3 < x_1 x_2^3$. △

We now define analogues of the univariate definitions such as the leading term of a polynomial:

Definition 3.14. Let $<$ be a term order on A and $f \in A$. We then define

- $\mathrm{LT}(f)$: the LEADING TERM of f is a term of the form cX for some non-zero $c \in k$ and $X \in \mathbb{T}^n$ that is $<$-maximal among the power products appearing in f.
- $\mathrm{LM}(f)$: the LEADING MONOMIAL is the power product of the leading term of f, that is, X.
- $\mathrm{LC}(f)$: the LEADING COEFFICIENT of f is the coefficient of $\mathrm{LT}(f)$, that is, c.
- $\mathrm{CT}(f)$: the CONSTANT TERM of f is the coefficient of the power product 1, that is, $\mathrm{CT}(f) = d$ for some $d \in k$ (if 1 does not occur as power product in f, we let $\mathrm{CT}(f) = 0$).

Example 3.15. Let $f = 2x^2 + 3xy^2 + 5y^3 + 1 \in \mathbb{Q}[x, y]$. Then, with lex and $x > y$, $\mathrm{LT}(f) = 2x^2$. With lex and $y > x$, $\mathrm{LT}(f) = 5y^3$. With deglex and $x > y$, $\mathrm{LT}(f) = 3xy^2$. The constant term of f is $\mathrm{CT}(f) = 1$. △

We can now formulate the concepts of reduction and a division algorithm in A. Let $<$ be a fixed term order on the monomials of A.

Definition 3.16. Given $f, g, h \in A$, we say that f REDUCES TO h BY g or write $f \xrightarrow{g} h$ if and only if $\mathrm{LT}(g)$ divides some non-zero term X in f and

$$h = f - \frac{X}{\mathrm{LT}(g)} g.$$

Let furthermore $F = \{f_1, \dots, f_s\} \subset A$ such that $f_i \neq 0$ for $i \in \{1, \dots, s\}$. We say that f REDUCES TO h MODULO F or write $f \xrightarrow{F}_+ h$ if and only if there exist a sequence $i_1, \dots, i_t \in \{1, \dots, s\}$ and a sequence $h_1, \dots, h_{t-1} \in A$ such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Example 3.17. Let $f = x^2y + yz$ and $G = \{g_1, g_2, g_3\}$ with $g_1 = xy$, $g_2 = y + z$ and $g_3 = z$. Since

$$\begin{array}{llll} h_1 & = f \;-\; \frac{x^2y}{\mathrm{LT}(g_1)} g_1 & = x^2y + yz - \frac{x^2y}{xy} xy & = yz \\ h_2 & = h_1 - \frac{yz}{\mathrm{LT}(g_2)} g_2 & = yz - \frac{yz}{y}(y + z) & = -z^2 \\ h_3 & = h_2 - \frac{-z^2}{\mathrm{LT}(g_3)} g_3 & = -z^2 + \frac{z^2}{\mathrm{LT}(z)} z & = 0, \end{array}$$

we can write $f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h_2 \xrightarrow{g_3} 0$ or $f \xrightarrow{G}_+ 0$. △

Definition 3.18. A polynomial $f \in A$ is said to be REDUCED with respect to $G = \{g_1, \dots, g_s\} \subset A$ if and only if $f = 0$ or if f is not reducible modulo G, that is, no term in f is divisible by $\mathrm{LT}(g_i)$ for $g \in \{1, \dots, s\}$.

We are now ready to formulate polynomial division in our setting, A:

Theorem 3.19. (*Multivariate polynomial division algorithm*) Given a polynomial $f \in A$ and a set of non-zero polynomials $G = \{g_1, \dots, g_s\} \subset A$, define the following algorithm:

1. If there exists $i \in \{1, \dots, s\}$ such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f)$, that is, if $\mathrm{LT}(f) = a\,\mathrm{LT}(g_i)$ for some a, add the a corresponding to the minimal such i to the quotient q_i and reiterate for

$$f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_i)} g_i = f - a g_i$$

2. If no such i exists, add $\mathrm{LT}(f)$ to the remainder r and reiterate for $f - \mathrm{LT}(f)$.

This algorithm terminates in a finite number of steps and produces quotients $q_1, \dots, q_s \in A$ and a remainder $r \in A$ that is reduced with respect to G so that

$$f = q_1 g_1 + \ldots + q_s g_s + r \quad \text{and} \quad \mathrm{LM}(f) = \max\left(\max_{1 \leq i \leq s} (\mathrm{LM}(q_i)\,\mathrm{LM}(g_i)), \mathrm{LM}(r) \right).$$

Proof. Label the polynomial at the start of the ith iteration of the algorithm by h_i. Then $\mathrm{LT}(h_i) > \mathrm{LT}(h_{i+1})$ and we obtain a descending chain of terms that terminates finitely by Theorem 3.7, proving the first assertion.

Furthermore, for any such h, $\mathrm{LM}(h) \leq \mathrm{LM}(h_1) = \mathrm{LM}(f)$. In this iteration we will add $-\frac{\mathrm{LT}(h)}{\mathrm{LT}(g_i)} g_i$ to h so that the leading term of h is cancelled and, consequently, add $\frac{\mathrm{LT}(h)}{\mathrm{LT}(g_i)}$ to q_i. Hence $\mathrm{LM}(q_i)\,\mathrm{LM}(g_i) \leq \mathrm{LM}(f)$.

From step 2 of the algorithm, it is clear that either $r = 0$ or no term in r is divisible by any $\mathrm{LM}(g_i)$ so that r is reduced with respect to G. □

A natural question is that of ideal membership, that is, if a given $f \in A$ is a member of some given ideal $I = (g_1, \dots, g_s) \trianglelefteq A$. If, following division of f by $\{g_1, \dots, g_s\}$ the remainder r is zero, f can be written as $f = \sum_i q_i g_i$ so that $f \in I$. However, the converse is not true in general: neither the quotients q_i nor the remainder r of a multivariate polynomial division are unique, as demonstrated in the following simple example. This will be one of the main motivations for introducing the concept of Gröbner bases in Section 3.2.

Example 3.20. Consider the ideal $I = (f_1, f_2) = (x^2 - x, x^2)$. The GCD of f_1 and f_2 is x. Since $f_2 - f_1 = x$, x is also a member of I. In fact, we see that $I = (x)$. The fact that x is an element of I cannot be derived via polynomial division of x by f_1 and f_2 since x is reduced with respect to $\{f_1, f_2\}$. △

3.2. Gröbner bases

The following definition will allow us to more easily formulate some of the statements of this section.

Definition 3.21. Let $S \subseteq A$. We define $\mathrm{LT}(S)$, the LEADING TERM IDEAL of S to be the ideal generated by the leading terms of the elements of S so that

$$\mathrm{LT}(S) = (\mathrm{LT}(p) \mid p \in S).$$

We now have all the tools required to formulate the definition of a particularly "well-behaved" set of generators of an ideal I that will allow us to algorithmically answer questions such as the one regarding ideal membership. Firstly we show the equivalence of four statements to which we shall adjoin one other later in this section.

Theorem 3.22. Let I be an ideal of A and G be a set of non-zero polynomials $G = \{g_1, \dots, g_s\} \subseteq I$. The following statements are equivalent:

(1) For all $f \in I$ such that $f \neq 0$, there exists $i \in \{1, \dots, s\}$ such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f)$.

(2) $f \in I$ if and only if $f \xrightarrow{G}_+ 0$.

(3) $f \in I$ if and only if $f = \sum_i q_i g_i$ with $\mathrm{LM}(f) = \max_i(\mathrm{LM}(q_i)\,\mathrm{LM}(g_i))$.

(4) $\mathrm{LT}(G) = \mathrm{LT}(I)$.

Proof. Assume (1) and let $f \in I$. Then $f \xrightarrow{G}_+ r$ for some r reduced with respect to G by the division algorithm of Theorem 3.19 so that $f - r \in I$ and $f \in I$ if and only if $r \in I$. Hence if $r = 0$, then $f \in I$. Conversely, assume that $f \in I$ and $r \neq 0$. Since $r \in I$, by (1) some $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(r)$ which is a contradiction of r being reduced. This proves (1) ⇒ (2).

Assume (2) and let $f \in I$. Then $f \xrightarrow{G}_+ 0$ and by Theorem 3.19, which is a reduction, we have

$$\mathrm{LM}(f) = \max_{1 \leq i \leq s} (\mathrm{LM}(q_i)\,\mathrm{LM}(g_i)),$$

so that (2) ⇒ (3).

Assume (3) and let $f \in I$. Then, since $f = \sum_i q_i g_i$,

$$\mathrm{LT}(f) = \sum_{\mathrm{LM}(q_i)\,\mathrm{LM}(g_i) = \mathrm{LM}(f)} \mathrm{LT}(q_i)\,\mathrm{LT}(g_i).$$

Thus $\mathrm{LT}(f) \in \mathrm{LT}(G)$ and since $\mathrm{LT}(I)$ is generated by the leading terms of the elements of I, we have shown $\mathrm{LT}(G) \supseteq \mathrm{LT}(I)$. The reverse inclusion is obvious. Hence (3) ⇒ (4).

Assume (4) and let $f \in I$ so that $\mathrm{LT}(f) \in \mathrm{LT}(I) = \mathrm{LT}(G)$ and $\mathrm{LT}(f) = \sum_i h_i \,\mathrm{LT}(g_i)$. Thus every term on the right-hand side is divisible by some $\mathrm{LM}(g_i)$, $i \in \{1, \dots, s\}$, so that $\mathrm{LM}(f)$ is divisible by some $\mathrm{LM}(g_i)$. Hence (4) ⇒ (1). □

Definition 3.23. A subset of non-zero polynomials $G = \{g_1, \dots, g_s\} \subseteq I$ satisfying any of the equivalent conditions of Theorem 3.22 is said to be a GRÖBNER BASIS of I.

Corollary 3.24. If $G = \{g_1, \dots, g_s\} \subseteq I$ is a Gröbner basis of I, then $I = (g_1, \dots, g_s)$.

Proof. The $\supseteq$ statement follows from the fact that G is a subset of I. For the other inclusion, $f \xrightarrow{G}_+ 0$ if $f \in I$ by Theorem 3.22 so that $I \subseteq (g_1, \dots, g_s)$. □

We see that a Gröbner basis $G \subseteq I$ generates the ideal I. Condition (2) of Theorem 3.22 then exactly answers the question of ideal membership discussed above. In fact, we can extend this statement in the following way:

Theorem 3.25. Let G be a Gröbner basis. For all $f \in A$, the remainder r obtained as $f \xrightarrow{G}_+ r$, where r is reduced with respect to G is unique.

Proof. Let $f \in A$ and let $f \xrightarrow{G}_+ r$ and $f \xrightarrow{G}_+ r'$ using polynomial division for remainders r, r' reduced with respect to G so that $f - r, f - r' \in I$. Then $(f - r') - (f - r) = r - r' \in I$ is reduced with respect to G. Unless $r - r' = 0$, this is a contradiction of statement (2) of Theorem 3.22. Hence $r = r'$ and the remainder is unique. □

Remark. In fact, the converse of the statement is true for a set $G = \{g_1, \dots, g_s\}$ of non-zero polynomials. Hence the property of the polynomial division remainder being unique can be taken as another condition equivalent to G being a Gröbner basis and appended to the list in Theorem 3.22. This is not necessary for our exposition. For a proof, see [AL94].

Having shown the beneficial properties of Gröbner bases, we establish existence:

Theorem 3.26. Any non-zero ideal I of A has a Gröbner basis.

Proof. Consider $\mathrm{LT}(I)$, the ideal generated by the leading terms of the elements of I.

Let $f \in \mathrm{LT}(I)$. Then

$$f = \sum_{i=1}^{\ell} c_i h_i X_i$$

for some $\ell \in \mathbb{N}$, some $h_i \in A$ and the leading terms $c_i X_i$ of some polynomials in I. Since every term on the right-hand side is divisible by an X_i, so is every term in f on the left-hand side.

By the Hilbert Basis Theorem (Theorem 2.20), $\mathrm{LT}(I)$ is finitely generated as an ideal of A, say $\mathrm{LT}(I) = (f_1, \ldots, f_n)$ for some $n \in \mathbb{N}$ and $f_i \in \mathrm{LT}(I)$. Then every term in f_i for $i \in \{1, \ldots, n\}$ is divisible by some $\mathrm{LT}(g_j)$, the leading term of some polynomial g_j in I by the argument above. Collecting these s leading terms and letting $G = \{g_1, \ldots, g_s\}$ we see that $\mathrm{LT}(G) = \mathrm{LT}(I)$ so that G is a Gröbner basis of I by Theorem 3.22. □

3.3. Buchberger's algorithm

In order to make use of the useful properties of Gröbner bases demonstrated in the previous section, an algorithmic method of constructing a Gröbner basis given a set of generators of an ideal I is needed. We begin by constructing a mechanism that accounts for cancellation of the leading terms of two polynomials. This construction will turn out to have more important repercussions than first may seem, as we shall see in Section 4.

Definition 3.27. Let f, g be two non-zero polynomials in A. We define $L = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$ to be the least common multiple of the leading power products of f and g, respectively. The S-POLYNOMIAL of f and g is then defined as

$$S(f, g) = \frac{L}{\mathrm{LT}(f)} f - \frac{L}{\mathrm{LT}(g)} g.$$

We now present another equivalent criterion for a subset G of I to be a Gröbner basis, given in terms of the S-polynomials.

Theorem 3.28. (*Buchberger's criterion*) A subset of non-zero polynomials $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for the ideal it generates if and only if

$$S(g_i, g_j) \xrightarrow{G}_+ 0 \quad \text{for all } i \neq j.$$

Lemma 3.29. Let $\{f_1, \ldots, f_s\} \subset A$ be a set of non-zero polynomials such that $\mathrm{LM}(f_i) = X$ for all $i \in \{1, \ldots, s\}$ and some $X \in \mathbb{T}^n$. Construct for some coefficients $c_i \in k$, $i \in \{1, \ldots, s\}$, the k-linear combination $f = \sum_i c_i f_i$. If $\mathrm{LM}(f) < X$, then f can be written as a k-linear combination of $S(f_i, f_j)$ for $1 \leq i < j \leq s$.

Proof. Let $\mathrm{LT}(f_i) = a_i X$ for $i \in \{1, \ldots, s\}$. We see that

$$S(f_i, f_j) = \frac{X}{a_i X} f_i - \frac{X}{a_j X} f_j = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j.$$

We can write

$$f = \sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i a_i \frac{1}{a_i} f_i = \sum_{i=1}^{s} \left(\sum_{j=1}^{i} c_j a_j - \sum_{j=1}^{i-1} c_j a_j \right) \frac{1}{a_i} f_i =$$
$$= \sum_{i=1}^{s-1} \left[\left(\sum_{j=1}^{i} c_j a_j - \sum_{j=1}^{i-1} c_j a_j \right) \left(\frac{1}{a_i} f_i + \frac{1}{a_{i+1}} f_{i+1} - \frac{1}{a_{i+1}} f_{i+1} \right) \right] + \left(\sum_{j=1}^{s} c_j a_j - \sum_{j=1}^{s-1} c_j a_j \right) \frac{1}{a_s} f_s =$$
$$= \sum_{i=1}^{s-1} \left[\left(\sum_{j=1}^{i} c_j a_j \right) \left(\frac{1}{a_i} f_i - \frac{1}{a_{i+1}} f_{i+1} \right) \right] + c_s a_s \frac{1}{a_s} f_s + M,$$

where

$$M = \sum_{i=1}^{s-1} \left[\left(\sum_{j=1}^{i} c_j a_j \right) \frac{1}{a_{i+1}} f_{i+1} \right] - \sum_{i=1}^{s-1} \left[\left(\sum_{j=1}^{i-1} c_j a_j \right) \frac{1}{a_i} f_i \right] =$$
$$= \sum_{i=1}^{s-2} \left[\left(\sum_{j=0}^{i} c_j a_j \right) \frac{1}{a_{i+1}} f_{i+1} \right] + \left(\sum_{j=1}^{s-1} c_j a_j \right) \frac{1}{a_s} f_s - \sum_{i=1}^{s-1} \left[\left(\sum_{j=0}^{i-1} c_j a_j \right) \frac{1}{a_i} f_i \right] = \left(\sum_{j=1}^{s-1} c_j a_j \right) \frac{1}{a_s} f_s,$$

so that

$$f = \sum_{i=1}^{s-1} \left[\left(\sum_{j=1}^{i} c_j a_j \right) \left(\frac{1}{a_i} f_i - \frac{1}{a_{i+1}} f_{i+1} \right) \right] + \left(\sum_{j=1}^{s} c_j a_j \right) \frac{1}{a_s} f_s = \sum_{i=1}^{s-1} \left(\sum_{j=1}^{i} c_j a_j \right) S(f_i, f_{i+1}),$$

since the assumption was that $c_1 a_1 + \ldots + c_s a_s = 0$. □

We now prove Theorem 3.28:

Proof. Let G be a Gröbner basis of $(g_1, \ldots, g_s) = I$. Then $S(g_i, g_j) \in I$ for all $i \neq j$ so that $S(g_i, g_j) \xrightarrow{G}_+ 0$ by Theorem 3.22.

For the converse statement, assume that $S(g_i, g_j) \xrightarrow{G}_+ 0$ for all $i \neq j$ and let $f \in I$. Among the representations of f as $f = \sum_i h_i g_i$, choose one such that $X = \max_i(\mathrm{LM}(h_i)\,\mathrm{LM}(g_i))$ is $<$-minimal by Theorem 3.7. We show that condition (3) of Theorem 3.22 is satisfied.

If $\mathrm{LM}(f) = X$, we are done. Otherwise $\mathrm{LM}(f) < X$. Denote by S the set of indices i such that $\mathrm{LM}(h_i)\,\mathrm{LM}(g_i) = X$ and let $\mathrm{LT}(h_i) = c_i X_i$. Construct now $g = \sum_{i \in S} c_i X_i g_i$ and let $r = f - g$. Then $\mathrm{LM}(X_i g_i) = X$ for $i \in S$ and $\mathrm{LM}(g) < X$, fulfilling the conditions of Lemma 3.29 so that we can express g as

$$g = \sum_{i<j \in S} d_{ij} S(X_i g_i, X_j g_j)$$

for some coefficients $d_{ij} \in k$. Explicitly, $\mathrm{LCM}(\mathrm{LM}(X_i g_i), \mathrm{LM}(X_j g_j)) = X$ and

$$S(X_i g_i, X_j g_j) = \frac{X}{\mathrm{LT}(X_i g_i)} X_i g_i - \frac{X}{\mathrm{LT}(X_j g_j)} X_j g_j = \frac{X}{\mathrm{LT}(g_i)} g_i - \frac{X}{\mathrm{LT}(g_j)} g_j = \frac{X}{L_{ij}} S(g_i, g_j),$$

where $L_{ij} = \mathrm{LCM}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$. Since we assume $S(g_i, g_j) \xrightarrow{G}_+ 0$ for $i \neq j$, using the same sequences in the reduction yields $S(X_i g_i, X_j g_j) \xrightarrow{G}_+ 0$ so that

$$S(X_i g_i, X_j g_j) = \sum_{k=1}^{s} h_{ijk} g_k$$

where, by the division algorithm (Theorem 3.19),

$$\max_{1\leq k\leq s}\big(\mathrm{LM}(h_{ijk})\,\mathrm{LM}(g_k)\big) = \mathrm{LM}(S(X_ig_i, X_jg_j)) < \mathrm{LCM}(\mathrm{LM}(X_ig_i), \mathrm{LM}(X_jg_j)) = X.$$

From this, it is clear that

$$f = g + r = \sum_{i<j\in S} d_{ij}S(X_ig_i, X_jg_j) + \sum_i a_ig_i = \sum_{i<j\in S} d_{ij}\sum_k h_{ijk}g_k + \sum_i a_ig_i = \sum_i b_ig_i$$

gives a representation $f = \sum_i b_ig_i$ where $\mathrm{LM}(b_i)\,\mathrm{LM}(g_i) < X$ for all $i \in \{1, \dots, s\}$, contradicting the minimality of the representation chosen above. Therefore $\mathrm{LM}(f) = X$ and we are done. □

From Theorem 3.28 an algorithm for computing a Gröbner basis given an initial set of polynomials generating I can be naturally formulated.

Proposition 3.30. (*Buchberger's algorithm*) Given a set $F = \{f_1, \dots, f_s\} \subset A$ of non-zero polynomials, let $G = F$ and collect the pairs $\{f, g\}$ for $f, g \in G$ such that $f \neq g$. Define the following algorithm:

1. Remove a pair $\{f, g\}$ from the set of pairs and let $S(f, g) \xrightarrow{G}_+ h$ so that h is reduced with respect to G
2. If $h \neq 0$, add all pairs $\{u, h\}$ for $u \in G$ to the set of pairs, add h to G and reiterate.

This algorithm terminates in a finite number of steps and produces a Gröbner basis G for the ideal $I = (f_1, \dots, f_s)$.

Proof. Assume that the algorithm does not terminate. Then in the ith iteration the algorithm will produce a set G_{i+1} such that $G_i \subsetneq G_{i+1}$ by adding to G_i an h_i that is reduced with respect to G_i. That is, no term in h_i is divisible by any $\mathrm{LT}(g_j)$ for $j \in \{1, \dots, s_i\}$. In particular, $\mathrm{LT}(h_i) \notin \mathrm{LT}(G_i)$ so that we obtain a strictly increasing chain of leading term ideals

$$\mathrm{LT}(G_1) \subsetneq \mathrm{LT}(G_2) \subsetneq \mathrm{LT}(G_3) \subsetneq \cdots,$$

contradicting the Noetherianity of A by the Hilbert Basis Theorem (Theorem 2.20).

For any $g_i, g_j \in G$, $S(g_i, g_j) \xrightarrow{G}_+ 0$ so that $G = \{g_1, \dots, g_t\}$ is a Gröbner basis of $(g_1, \dots, g_t)$. Evidently, $F \subseteq G$ so that $(f_1, \dots, f_s) \subseteq (g_1, \dots, g_t)$. Any h_i added to G_i in the ith iteration of the algorithm is certainly in $(f_1, \dots, f_s)$ so that $I = (f_1, \dots, f_s) = (g_1, \dots, g_t)$ and G is a Gröbner basis of I. □

Example 3.31. We now return to the example 2.27 from section 2.3 with the circle and ellipse described by the equations $x^2 + y^2 = 1$ and $\frac{1}{3}x^2 + 3y^2 = 1$. Consider the ideal $(x^2 + y^2 - 1, \frac{1}{3}x^2 + 3y^2 - 1)$ under a lex ordering with $x > y$.

Let $h_1 = x^2 + y^2 - 1$ and $h_2 = \frac{1}{3}x^2 + 3y^2 - 1$ and $G_1 = \{h_1, h_2\}$.

Construct $S(h_1, h_2) = -\frac{8}{3}y^2 + \frac{2}{3}$. Then $S(h_1, h_2)$ is reduced with respect to G_1. Set $S(h_1, h_2) = h_3$ and let $G_2 = \{h_1, h_2, h_3\}$.

Construct $S(h_1, h_3) = -\frac{2}{3}x^2 - \frac{8}{3}y^4 + \frac{8}{3}y^2$. Then $S(h_1, h_3) \xrightarrow{G_2}_+ 0$.

Construct $S(h_2, h_3) = -\frac{2}{9}x^2 - 8y^4 + \frac{8}{3}y^2$. Then $S(h_2, h_3) \xrightarrow{G_2}_+ 0$.

Thus G_2 is a Gröbner basis for the ideal. △

3.4. Uniqueness, some examples and applications

Proposition 3.32. Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for an ideal I. If $\mathrm{LM}(g_2)$ divides $\mathrm{LM}(g_1)$, then $\{g_2, \ldots, g_s\}$ is a Gröbner basis for I.

Proof. We use the first condition of Theorem 3.22. Let $f \in I$ be a polynomial such that $\mathrm{LM}(g_1)$ divides $\mathrm{LM}(f)$. Then $\mathrm{LM}(g_2)$ divides $\mathrm{LM}(f)$. □

Definition 3.33. A Gröbner basis $G = \{g_1, \ldots, g_s\}$ is said to be MINIMAL if $\mathrm{LC}(g_i) = 1$ for all i and no $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(g_j)$ for $i \neq j$.

Remark. A minimal Gröbner basis is only minimal in the sense that no leading terms of basis elements divide one another. A further restriction on a Gröbner basis yielding a generating set of minimal cardinality will be given below as terming the Gröbner basis *reduced*.

The following lemma will be useful in showing the uniqueness of a certain type of Gröbner bases to be defined shortly.

Lemma 3.34. If $F = (f_1, \ldots, f_s)$ and $G = (g_1, \ldots, g_t)$ are two minimal Gröbner bases of I, then $s = t$ and $\mathrm{LT}(f_i) = \mathrm{LT}(g_i)$ after renumbering.

Proof. Since $f_1 \in I$, there exists an $i \in \{1, \ldots, t\}$ such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f_1)$. Reorder G so that $i = 1$. Since $g_1 \in I$, there exists $j \in \{1, \ldots, s\}$ such that $\mathrm{LM}(f_j)$ divides $\mathrm{LM}(g_1)$. But then $\mathrm{LM}(f_j)$ divides $\mathrm{LM}(f_1)$ and F is minimal, so $j = 1$ and $\mathrm{LM}(f_1) = \mathrm{LM}(g_1)$.

Since $f_2 \in I$, there exists $i \in \{1, \ldots, t\}$ such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f_2)$ and $i \neq 1$ since F is minimal. Reorder G so that $i = 2$. By the same reasoning as above, $\mathrm{LM}(f_2) = \mathrm{LM}(g_2)$. Continuing this process until all elements of F and G have been considered, we arrive at the conclusion $|F| = s = t = |G|$ and $\mathrm{LT}(f_i) = \mathrm{LT}(g_i)$ after renumbering. □

We can now formulate a restriction on a Gröbner basis for an ideal I so that I can be uniquely described by a Gröbner basis of this type.

Definition 3.35. A Gröbner basis $G = \{g_1, \ldots, g_s\}$ is said to be REDUCED if $\mathrm{LC}(g_i) = 1$ and g_i is reduced with respect to $G \setminus \{g_i\}$ for all i.

Remark. In particular, a reduced Gröbner basis is minimal.

What follows is a method for constructing a reduced Gröbner basis for an ideal, showing existence.

Proposition 3.36. Given a minimal Gröbner basis $G = \{g_1, \ldots, g_s\}$ of an ideal I, define the following algorithm for $i \in \{1, \ldots, s\}$:

1. Construct $H_i = \{h_1, \ldots, h_{i-1}, g_{i+1}, \ldots, g_s\}$
2. Obtain h_i by $g_i \xrightarrow{H_i}_+ h_i$ so that h_i is reduced with respect to H_i.

This algorithm yields a reduced Gröbner basis $H = \{h_1, \ldots, h_s\}$ for I.

Proof. Since G was minimal, the leading term of every g_i will be in the output of the reduction, h_i so that $\mathrm{LM}(h_i) = \mathrm{LM}(g_i)$ and H is a minimal Gröbner basis by Theorem 3.22.

Furthermore, since h_i is reduced with respect to H_i, no term in h_i is divisible by any of the terms

$$\{\mathrm{LM}(h_1), \ldots, \mathrm{LM}(h_{i-1}), \mathrm{LM}(g_{i+1}), \ldots, \mathrm{LM}(g_s)\} = \{\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_{i-1}), \mathrm{LM}(g_{i+1}), \ldots, \mathrm{LM}(g_s)\}$$

so that h_i is indeed reduced with respect to $G \setminus \{g_i\}$ and H is a reduced Gröbner basis of I. □

Example 3.37. Returning to the circle and ellipse of the examples 2.27 and 3.31 we will now present a reduction. Multiplying to get monic leading terms, set $G_3 = \{x^2+y^2-1, x^2+9y^2-3, y^2-1/4\}$. Since $\mathrm{LT}(g_1) = x^2$ divides $\mathrm{LT}(g_2) = x^2$, we can discard the middle polynomial and set $G_4 = \{x^2+y^2-1, y^2-\frac{1}{4}\}$. This is a minimal Gröbner basis. Continuing our reduction,

$$x^2+y^2-1 \xrightarrow{G_4 \setminus \{h_1\}}_+ x^2 - \frac{3}{4}.$$

No further reductions can be made and we have the reduced Gröbner basis $G = \{g_1, g_2\}$ with

$$g_1 = y^2 - 1/4$$
$$g_2 = x^2 - 3/4.$$

△

Theorem 3.38. (*Buchberger*) For a fixed term order $<$ on $\mathbb{T}^n$, every non-zero ideal I of A has a unique reduced Gröbner basis with respect to $<$.

Proof. Assume that G and H are two reduced, and thus minimal, Gröbner bases of I. Then $|G| = |H| = s$ and we can assume $\mathrm{LT}(g_i) = \mathrm{LT}(h_i)$, $i \in \{1, \ldots, s\}$, by Lemma 3.34.

For such an i, assume that $g_i \neq h_i$. Then $g_i - h_i \in I$ and so there exists j such that $\mathrm{LM}(h_j)$ divides $\mathrm{LM}(g_i - h_i)$ (since H is a Gröbner basis of I), so that $\mathrm{LM}(h_j) \leq \mathrm{LM}(g_i - h_i)$ by Lemma 3.6. Since $\mathrm{LM}(g_i - h_i) < \mathrm{LM}(h_i)$, we can state that $j \neq i$. Then $\mathrm{LM}(h_j) = \mathrm{LM}(g_j)$ divides some term in h_i or g_i, contradicting the reducedness of G and H. Hence $g_i = h_i$. □

3.5. Another example: the elementary symmetric polynomials

A polynomial which is invariant under permutation of the variables is called symmetric. The polynomial $x^2 + xy + y^2$ is an example of a symmetric polynomial in x and y. These polynomials appear naturally in the study of roots to polynomial equations and in Galois theory. The theory of symmetric polynomials is also deeply interconnected with other areas of mathematics, such as representation theory and combinatorics. In some sense, the most simple symmetric polynomials are the elementary symmetric polynomials, defined as follows.

Definition 3.39. The kth elementary symmetric polynomial in n variables is defined by

$$\sigma_{k,n} = \sum_{1 \leq j_1 < \ldots < j_k \leq n} x_{j_1} x_{j_2} \cdots x_{j_k}.$$

Example 3.40. For one variable, $n = 1$, the elementary symmetric polynomials are

$$\sigma_{1,1} = x_1.$$

For $n = 2$,

$$\sigma_{1,2} = x_1 + x_2$$
$$\sigma_{2,2} = x_1 x_2.$$

For $n = 3$,

$$\sigma_{1,3} = x_1 + x_2 + x_3$$
$$\sigma_{2,3} = x_1 x_2 + x_1 x_3 + x_2 x_3$$
$$\sigma_{3,3} = x_1 x_2 x_3.$$

△

The symmetric polynomials in any commutative polynomial ring constitute a ring (see [BW93] for reference) that is customarily denoted by $R[x_1, \ldots, x_n]^S$. Clearly the elementary symmetric polynomials all lie in this ring - in fact, every symmetric polynomial can be written as a polynomial in the elementary symmetric polynomials. A well-known result called the fundamental theorem of symmetric polynomials captures this fact.

Theorem 3.41. (*Fundamental theorem of symmetric polynomials*) For a commutative ring R, the ring of symmetric polynomials in n variables is isomorphic to the ring of polynomials in the elementary symmetric polynomials: $R[x_1, \ldots, x_n]^S \cong R[y_1, \ldots, y_n]$, where the isomorphism sends any $\sigma_{j,n}$ to y_j. That is, any $f \in R[x_1, \ldots, x_n]^S$ can be written as $f = g(\sigma_{1,n}, \ldots, \sigma_{n,n})$ in a unique way for a $g \in R[y_1, \ldots, y_n]$.

Proof. This can be shown with the theory of term orders, as is done in for example [BW93] or [CLO07]. It can also be proven via Galois theory, for which we refer the reader to [DF04]. □

Let us now again consider the ring $k[x_1, ..., x_n]$. Since a Gröbner basis will give us computational benefits and possibilites, we intend to present a Gröbner basis (for the lex ordering $x_n > x_{n-1} > \cdots > x_1$) for the ideal generated by the elementary symmetric polynomials, $(\sigma_{1,n}, \ldots, \sigma_{n,n})$.

Definition 3.42. We define the complete symmetric sums $h_{d,m}$ by

$$h_{d,m} = \sum_{a_1+\ldots+a_m=d} x_1^{a_1} \cdots x_m^{a_m}.$$

Definition 3.43. We define the gröbnerian symmetric sums $g_{d,n}$ by

$$g_{d,n} = h_{d,n-d+1}.$$

Examples 3.44. For one variable, $n = 1$, we have

$$g_{1,1} = x.$$

For $n = 2$, we have

$$g_{1,2} = x + y$$
$$g_{2,2} = x^2.$$

For $n = 3$, we have

$$g_{1,3} = x + y + z$$
$$g_{2,3} = x^2 + xy + y^2$$
$$g_{3,3} = x^3.$$

△

Proposition 3.45. The formula

$$\sigma_{d,n} + (-1)^d g_{d,n} + \sum_{k=1}^{d-1} (-1)^k g_{k,n} \sigma_{d-k,n-k} = 0 \tag{1}$$

holds. This is proven by elementary inductive techniques in [MS03]. This formula can be considered a late addition to the well-known and similar Newton-Girard identities (see [Mea92]).

Proposition 3.46. $(g_{1,n}, \ldots, g_{n,n}) = (\sigma_1, \ldots, \sigma_n)$.

Proof. This proof is a slight simplification of a more general result for other families of symmetric functions shown in [MS03].

First, we can rewrite (1) on the following form, with $c_k = (-1)^{k+1}\sigma_{d-k,n-k}$ for $k < d-1$ and $c_d = (-1)^{d+1}$:

$$\sigma_{d,n} = \sum_{j=1}^{d} c_j g_{j,n}$$

and directly note that the inclusion $(\sigma_{1,n}, \dots, \sigma_{n,n}) \subseteq (g_1, \dots, g_n)$ holds.

Second, we will show the other inclusion by induction. For the base case, we note that $g_1 \in (g_1) = (\sigma_1)$. Now assume that $\{g_1, \dots, g_{j-1}\} \subset (\sigma_{1,n}, \dots, \sigma_{j-1,n})$.

Rearranging (1) it is clear that $g_j \in (g_1, \dots, g_{j-1}, \sigma_{j,n}) \subseteq (\sigma_{1,n}, \dots, \sigma_{j,n})$, proving the equality. □

Corollary 3.47. Since $\mathrm{LT}(g_{k,n}) = x_{n-k+1}^k$, and in particular since $\mathrm{LT}(g_k)$ does not divide $\mathrm{LT}(g_j)$ for $j \neq k$, the set $\{g_{j,n}\}$ gives a Gröbner basis for the ideal generated by the elementary symmetric polynomials. Since the g_i are monic and no leading term of any g_i divides any of the terms of another, the basis is also reduced.

4. Modules and Gröbner bases

We continue to follow the exposition and definitions of [AL94], unless otherwise specified. Some steps in proofs have been elaborated upon for clarity.

4.1. Modules: some definitions

Modules were introduced by Emmy Noether as a common generalization of ideals and vector spaces and are now one of the standard tools used in algebra. In this chapter we present the basic theory of modules, many of these definitions closely following the ring properties treated in earlier sections. In the following section we present a natural generalization of Gröbner theory to submodules of modules over polynomial rings. This extension has become standard and can be used to prove some previously non-constructive results in a constructive way.

Definition 4.1. Given a commutative ring R, an abelian group $(M, +)$ and an operation $R \times M \to M$, M is said to be an R-MODULE if for all $\mathbf{m}, \mathbf{n} \in M$ and $r, s \in R$,

- $r(\mathbf{m} + \mathbf{n}) = r\mathbf{m} + r\mathbf{n}$
- $(r + s)\mathbf{m} = r\mathbf{m} + s\mathbf{m}$
- $(rs)\mathbf{m} = r(s\mathbf{m})$
- $1_R\mathbf{m} = \mathbf{m}$.

Remark. If k is a field, a k-module is called a *vector space.*

Definition 4.2. A subset $N \subseteq M$ that is in itself an R-module is said to be a SUBMODULE of M, written $N \leq M$. If furthermore every $\mathbf{n} \in N$ can be written as $\mathbf{n} = r_1\mathbf{a}_1 + \ldots + r_t\mathbf{a}_t$ for $r_i \in R$, the GENERATING SET $\{\mathbf{a}_1, \ldots, \mathbf{a}_t\} \subseteq N$ and $i \in \{1, \ldots, t\}$, we say N is FINITELY GENERATED. We then write $N = \langle \mathbf{a}_1, \ldots, \mathbf{a}_t \rangle$.

Definition 4.3. A module is said to be FREE if there exists a generating set or basis $B \subseteq M$ such that every element $\mathbf{m} \in M$ can be written as a finite sum

$$\mathbf{m} = \sum_{i=1}^{s} r_i \mathbf{b}_i$$

in a unique way with coefficients $r_i \in R$ and basis elements $\mathbf{b}_i \in B$.

Example 4.4. The polynomial ring A is in itself an A-module with the usual multiplication between elements of A. Considering A as an A-module in this sense, we will denote it by A^1. The submodules of A^1 are then exactly the ideals of A, closed under multiplication by elements of A. A basis for A^1 is the set $\{1\}$, so A^1 is free. △

Definition 4.5. A HOMOMORPHISM (of R-modules) is a function $\phi : M \to M'$ between two R-modules M, M' such that:

- *Additivity:* for all $\mathbf{m}, \mathbf{n} \in M$, $\phi(\mathbf{m} + \mathbf{n}) = \phi(\mathbf{m}) + \phi(\mathbf{n})$.
- *Compatibility:* for all $\mathbf{m} \in M$ and $r \in R$, $r\phi(\mathbf{m}) = \phi(r\mathbf{m})$.

A bijective homomorphism is said to be an ISOMORPHISM. Importantly, any homomorphism factors through an isomorphism:

Theorem 4.6. (*The first isomorphism theorem for modules*) For any homomorphism $\phi : M \to N$ the kernel $\ker \phi$ is a submodule of M, the image $\operatorname{im} \phi$ is a submodule of N and we have an isomorphism:

$$M/\ker \phi \cong \operatorname{im} \phi.$$

We now introduce the analogue of Definition 2.16.

Definition 4.7. A module M is said to be NOETHERIAN if every submodule $N \leq M$ is finitely generated or, equivalently, if for an ascending chain of submodules $N_i \leq M$

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$$

there exists n such that for $i \geq n$, $N_i = N_n$.

Let now $A = k[x_1, \ldots, x_n]$ and consider for $s \in \mathbb{N}$ the cartesian product A^s. We denote an element $\mathbf{m} \in A^s$ by $\mathbf{m} = (m_1, \ldots, m_s)$ (this is not to be confused with the notation used for a finitely generated ideal). Then A^s with the following notion of scalar multiplication $A \times A^s \to A^s$:

$$p\mathbf{m} = p(m_1, \ldots, m_s) = (pm_1, \ldots, pm_s)$$

is a free A-module with the finite *standard basis* $\{\mathbf{e}_i\}_{i=1}^s$, where a basis element $\mathbf{e}_i$ is zero at all components except for being 1 at its ith component. Abusing terminology we sometimes call an element $\mathbf{m} \in A^s$ a *vector*, despite A^s not being a vector space (since the ring of scalars $k[x_1, \ldots, x_n]$ is not a field).

We observe that for a homomorphism between free A-modules, the map is defined by the images of the standard basis vectors of A^s, that is, by $\phi(\mathbf{e}_i) \in A^t$ for $i \in \{1, \ldots, s\}$. Therefore we can express ϕ in terms of matrix multiplication by the matrix that we will also refer to as ϕ by abuse of notation, $\phi : \mathbf{m} \mapsto \big(\phi(\mathbf{e}_1) \quad \cdots \quad \phi(\mathbf{e}_s)\big)\, \mathbf{m} = \phi\mathbf{m}$.

The Noetherian property of A as a ring allows us to show the following generalization of the Hilbert basis theorem (Theorem 2.20):

Proposition 4.8. A^s is Noetherian.

Proof. Let $M \leq A^s$. We show that M is finitely generated by induction on s.

If $s = 1$, then $A^s = A^1$ and $M \trianglelefteq A$. By Theorem 2.20, A is Noetherian as a ring and thus M is finitely generated.

Assume for the inductive step that $s > 1$ and that the submodules of A^{s-1} are finitely generated. Then

$$I = \{a \in A \,|\, a \text{ is the first coordinate of some } \mathbf{m} \in M\}$$

is an ideal of A, since M is a submodule of A^s, and is finitely generated by the Hilbert basis theorem so that $I = \langle a_1, \ldots, a_t \rangle$. Associate to each a_i its element $\mathbf{m}_i \in M$ as in the definition of I.

Let now

$$M' = \{(b_2, \ldots, b_m) \,|\, (0, b_2, \ldots, b_m) \in M\}.$$

Evidently $M' \leq A^{s-1}$ and is thus by induction finitely generated, $M' = \langle \mathbf{n}'_1, \ldots, \mathbf{n}'_\ell \rangle$. For $i \in \{1, \ldots, \ell\}$, let $\mathbf{n}_i = (0, n'_{i,1}, \ldots, n'_{i,s-1})$.

For $\mathbf{m} \in M$, we have that $m_1 = \sum_i r_i a_i$ for some $r_i \in A$ and $i \in \{1, \dots, t\}$. Furthermore, let $\mathbf{m}' = \mathbf{m} - \sum_i r_i \mathbf{m}_i$. Then $\mathbf{m}' \in M$ and $m_1' = 0$, so that $\mathbf{m}' = \sum_i p_i \mathbf{n}_i$. Hence

$$\mathbf{m} = \sum_{i=1}^{t} r_i \mathbf{m}_i + \sum_{i=1}^{\ell} p_i \mathbf{n}_i,$$

so that $M = \langle \mathbf{m}_1, \dots, \mathbf{m}_t, \mathbf{n}_1, \dots, \mathbf{n}_\ell \rangle$ and is finitely generated. □

Proposition 4.9. Given a finitely generated A-module M, there exist $s \in \mathbb{N}$ and a submodule $N \le A^s$ such that

$$M \cong A^s/N.$$

In particular, M is Noetherian.

Proof. Let M be an A-module and $\{\mathbf{m}_i\}_{i=1}^{s} \subseteq M$. Then the following map is a homomorphism:

$$\begin{array}{cccc} \phi: & A^s & \to & M \\ & (a_1, \dots, a_s) & \mapsto & \sum\limits_{i=1}^{s} a_i \mathbf{m}_i \end{array}$$

In particular, if $\{\mathbf{m}_i\}$ is chosen to be a generating set for M, ϕ is surjective. The conclusion follows from Theorem 4.6.

The second assertion follows from the fact that if $K \le M \cong A^s/N$, then $K \cong L/N$ for some $L \le A^s$. By Theorem 4.8, L is finitely generated and hence so is L/N, so that every submodule of M is finitely generated. □

Definition 4.10. If M is an A-module such that $M \cong A^s/N$ as in Proposition 4.9, then A^s/N is said to be the PRESENTATION of M.

Example 4.11. Consider the ground field k as an A-module with the following scalar multiplication:

$$\begin{array}{ccc} A \times k & \to & k \\ (p, r) & \mapsto & \mathrm{CT}(p)r. \end{array}$$

In order to present k as an A-module, we construct a surjective homomorphism $\phi : A \to k$ such that $1 \mapsto 1$ and $x_i \mapsto 0$. Then $\ker \phi = \langle x_1, \dots, x_n \rangle$. Then, by the isomorphism theorem 4.6 we obtain $k \cong A/\langle x_1, \dots, x_n \rangle$. △

Proposition 4.9 allows us to describe *any* finitely generated A-module in terms of the quotient of a free module with some submodule of said free module. This, together with the above mentioned fact that homomorphisms between free A-modules are easily described will allow for the computation of free resolutions in Section 4.3 and the formulation of methods for explicit computations of objects such as the *set of homomorphisms* Hom between two arbitrary A-modules in Sections 4.5 and 4.6.

4.2. Gröbner formulation in A^s

This section defines the machinery which will enable us to obtain a Gröbner basis theory with the theory presented in Section 3 obtained as a special case. To this end we require some definitions to be made so as to have meaningful analogues of concepts such as divisibility. For results that are straightforward analogues of their A^1 counterparts we omit proofs and refer to the original result proved in Section 3, replacing arguments using the Hilbert basis theorem (Theorem 2.20) with Proposition 4.8.

Definition 4.12. A TERM in A^s is a vector of the type $\mathbf{X} = cX\mathbf{e}_i$ for a coefficient $c \in k$, some power product $X \in \mathbb{T}^n$ and a basis vector $\mathbf{e}_i \in A^s$, $i \in \{1, \ldots, s\}$. If $c = 1$ we say that $\mathbf{X}$ is a MONOMIAL in A^s. For two terms $\mathbf{X} = cX\mathbf{e}_i, \mathbf{Y} = dY\mathbf{e}_j$ we say that $\mathbf{X}$ divides $\mathbf{Y}$ if and only if $i = j$ and X divides Y as a monomial in A. We define $\mathbf{Y}/\mathbf{X} = (d/c)(Y/X)$.

We now need a way to compare two vector monomials. To this end we extend the definition of term orders to A^s and state the term order most often used in this setting. As in the case of $s = 1$, any term order on the monomials of A^s satisfying the following definition will be a well-ordering (a direct analogue of Theorem 3.7). Abusing notation, we will denote a generic term order defined on A^s as $<$ for simplicity, distinguishing it from the term order $<$ defined on A only when necessary.

Definition 4.13. A TERM ORDER $<$ on the monomials of A^s is a total order $<$ that satisfies for all monomials $\mathbf{X}, \mathbf{Y} \in A^s$:

- $\mathbf{X} < Z\mathbf{X}$ for all power products $Z \neq 1$ in A
- If $\mathbf{X} < \mathbf{Y}$, then $Z\mathbf{X} < Z\mathbf{Y}$ for all power products Z in A.

Definition 4.14. The TERM OVER POSITION (TOP) term order on the monomials of A^s with $\mathbf{e}_1 < \mathbf{e}_2 < \cdots < \mathbf{e}_s$ is defined as follows: for monomials $\mathbf{X} = X\mathbf{e}_i$, $\mathbf{Y} = Y\mathbf{e}_j$ in A^s and a term order $<$ defined on A, we have that

$$\mathbf{X} < \mathbf{Y} \iff (X < Y) \text{ or } (X = Y \text{ and } i < j)\,.$$

In other words, this term order compares two vector terms by their A-monomials and breaks a tie by comparing indices of their respective basis vectors.

Example 4.15. With TOP lex, $x_1 > x_2$ and $\mathbf{e}_1 < \mathbf{e}_2$, we have

$$\mathbf{e}_1 < \mathbf{e}_2 < x_2\mathbf{e}_1 < x_2\mathbf{e}_2 < x_1\mathbf{e}_1 < x_1\mathbf{e}_2.$$

△

The following definitions echo their counterparts in A:

Definitions 4.16. Given a term order $<$ on the monomials of A^s and a vector $\mathbf{f} \in A^s$, we define the following:

- $\mathrm{LT}(\mathbf{f}) = a\mathbf{X}$ is the LEADING TERM of f
- $\mathrm{LM}(\mathbf{f}) = \mathbf{X}$ is the LEADING MONOMIAL of f
- $\mathrm{LC}(\mathbf{f}) = a$ is the LEADING COEFFICIENT of f
- For two monomials $\mathbf{X} = X\mathbf{e}_i$ in A^s, $\mathbf{Y} = Y\mathbf{e}_j$, we define the least common multiple

$$\mathrm{LCM}(\mathbf{X}, \mathbf{Y}) = \begin{cases} \mathbf{0} & \text{if } i \neq j \\ \mathrm{LCM}(X, Y)\mathbf{e}_i & \text{if } i = j \end{cases}$$

- Given a submodule $M \leq A^s$, $\mathrm{LT}(M) = \langle \mathrm{LT}(\mathbf{m}) \,|\, \mathbf{m} \in M \rangle \leq A^s$ is the LEADING TERM MODULE of M.

Example 4.17. Let $\mathbf{f} = (2x + y, 3x) \in A^2$ with TOP lex, $x > y$ and $\mathbf{e}_1 < \mathbf{e}_2$. Then $\mathrm{LT}(\mathbf{f}) = 3x\mathbf{e}_2$, $\mathrm{LM}(\mathbf{f}) = x\mathbf{e}_2$ and $\mathrm{LC}(\mathbf{f}) = 3$. Furthermore, the leading term module is given by $\mathrm{LT}(\{\mathbf{f}\}) = \langle (0, 3x) \rangle$. △

Proposition 4.18. The division algorithm in A^s mirrors the single-dimension case of generalized polynomial division exactly in that, given $\mathbf{f}$ and a set $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_t\} \subseteq A^s$, one obtains quotients $q_1, \ldots, q_t \in A$ and a remainder $\mathbf{r} \in A^s$ which is reduced with respect to F. One can thus write

$$\mathbf{f} = q_1\mathbf{f}_1 + \ldots + q_s\mathbf{f}_s + \mathbf{r}.$$

Before moving on to the definition of Gröbner bases and its application for more general purposes in Section 4.3 we consider the analogue of a particular aspect of the conventional theory - the S-polynomials - which, as we shall see, play a particular role in the module theory.

Definition 4.19. Given a Gröbner basis $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ of some submodule $M \leq A^s$, assuming that $\mathrm{LC}(\mathbf{g}_i) = 1$ and letting $\mathrm{LT}(\mathbf{g}_i) = \mathbf{X}_i$ for $i \in \{1, \ldots, t\}$, let $\mathbf{X}_{ij} = \mathrm{LCM}(\mathrm{LM}(\mathbf{g}_i), \mathrm{LM}(\mathbf{g}_j))$ and define

$$S(\mathbf{g}_i, \mathbf{g}_j) = \frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{g}_i - \frac{\mathbf{X}_{ij}}{\mathbf{X}_j}\mathbf{g}_j.$$

We can finally define the following, noting that the Buchberger algorithm given in Proposition 3.30 is completely equivalent,

Definition 4.20. A GRÖBNER BASIS for the submodule $M \leq A^s$ is a set of non-zero vectors $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\} \subseteq M$ satisfying any of the following equivalent conditions:

1. For all $\mathbf{f} \in M$ such that $\mathbf{f} \neq \mathbf{0}$, there exists $i \in \{1, \ldots, t\}$ such that $\mathrm{LM}(\mathbf{g}_i)$ divides $\mathrm{LM}(\mathbf{f})$.
2. $\mathbf{f} \in M$ if and only if $\mathbf{f} \xrightarrow{G}_+ \mathbf{0}$.
3. If $\mathbf{f} \in M$, then $f = \sum_i h_i\mathbf{g}_i$ with $\mathrm{LM}(f) = \max_i(\mathrm{LM}(h_i)\,\mathrm{LM}(\mathbf{g}_i))$.
4. $\mathrm{LT}(G) = \mathrm{LT}(M)$.
5. $S(\mathbf{g}_i, \mathbf{g}_j) \xrightarrow{G}_+ \mathbf{0}$ for all $i \neq j$.

Remark. Continuing the terminology from the case of A, calling this object a Gröbner *basis* has nothing to do with the notion of basis of a free module as in Definition 4.3.

The uniqueness of remainder after polynomial division with G as well as the results on existence and uniqueness of Gröbner bases also carry over from A^1.

4.3. Syzygies

In Section 4.1 we saw that an arbitrary finitely generated A-module M could be *presented* by letting M be the image of a homomorphism from a free module. We now define a particularly useful concept that will allow us to describe kernels of such homomorphisms, crucial for computations in modules:

Definition 4.21. Let $\{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subseteq A^m$. Then constructing a homomorphism

$$\begin{array}{cccc} \phi: & A^s & \to & A^m \\ & (a_1, \ldots, a_s) & \mapsto & \sum\limits_{i=1}^{s} a_i\mathbf{f}_i, \end{array}$$

the kernel of ϕ is a submodule of A^s and is said to be the SYZYGY MODULE of $\begin{pmatrix}\mathbf{f}_1 & \cdots & \mathbf{f}_s\end{pmatrix} \in A^{m\times s}$, $\mathrm{Syz}(\mathbf{f}_1, \ldots, \mathbf{f}_s) = \ker\phi \leq A^s$. We refer to the elements of the syzygy module as *syzygies.*

This is exactly the set of polynomial solutions $(h_1, \ldots, h_s) \in A^s$ to the following homogeneous linear equation with coefficients in A^m:

$$\mathbf{f}_1 h_1 + \ldots + \mathbf{f}_s h_s = \mathbf{0},$$

i.e. the set of linear dependences of the generators of M.

Remark. A result that is not used in this text but is nevertheless of interest is that given two ordered generating sets F and G of the same A-module M, there exist free A-modules L, L' such that $\operatorname{Syz}(F) \oplus L \cong \operatorname{Syz}(G) \oplus L'$. The full statement and proof can be found in, for instance, [CLO05].

Example 4.22. The ideal (x, y) of $A = k[x, y]$ can be regarded as a submodule $\langle x, y\rangle$ of A^1. For the generators x, y the linear combination $ax + by$ is zero if $a = cy$ and $b = -cx$ for some element c. Thus $(y, -x) \in A^2$ is an element of the syzygy module $\operatorname{Syz}(x, y)$. In fact, it is a generating element, so that $\operatorname{Syz}(x, y) = \langle (y, -x)\rangle$. △

We shall now see the role that S-polynomials play in terms of syzygies the Gröbner basis G:

Proposition 4.23. Let $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\} \subseteq A^m$ be a Gröbner basis of a submodule $M \leq A^m$. By condition (5) of Definition 4.16, $S(\mathbf{g}_i, \mathbf{g}_j) \xrightarrow{G}_+ \mathbf{0}$ for $i \neq j$, so that $S(\mathbf{g}_i, \mathbf{g}_j) = \sum_k h_{ijk}\mathbf{g}_k$ for $h_{ijk} \in A$ and $k \in \{1, \ldots, t\}$. Define

$$\mathbf{s}_{ij} = \frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{e}_i - \frac{\mathbf{X}_{ij}}{\mathbf{X}_j}\mathbf{e}_j - (h_{ij1}, \ldots, h_{ijt}) \quad \text{for} \quad 1 \leq i < j \leq t.$$

Then $H = \{\mathbf{s}_{ij} \mid 1 \leq i < j \leq t\} \subseteq A^t$ is a generating set for the syzygy module $\operatorname{Syz}(G)$.

Lemma 4.24. Let $\mathbf{X}_1, \ldots, \mathbf{X}_s$ be monomials in A^m so that $\mathbf{X}_i = X_i\mathbf{e}_j$ for some $j \in \{1, \ldots, m\}$. Then

$$C = \left\{ \mathbf{C}_{ij} = \frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{e}_i - \frac{\mathbf{X}_{ij}}{\mathbf{X}_j}\mathbf{e}_j \,\middle|\, i, j \in \{1, \ldots, s\} \right\}$$

is a generating set for the syzygy module $\operatorname{Syz}(\mathbf{X}_1, \ldots, \mathbf{X}_s)$.

Proof. First, for $i \neq j$, note that $\begin{pmatrix}\mathbf{X}_1 & \cdots & \mathbf{X}_s\end{pmatrix}\mathbf{C}_{ij} = \mathbf{0}$, mirroring the property of the original S-polynomials in A so that $\langle C\rangle \subseteq \operatorname{Syz}(\mathbf{X}_1, \ldots, \mathbf{X}_s)$.

Let $\mathbf{h} = (h_1, \ldots, h_s) \in \operatorname{Syz}(\mathbf{X}_1, \ldots, \mathbf{X}_s) \leq A^s$. We write the ith polynomial component of the syzygy $\mathbf{h}$ as the sum of its terms $h_i = \sum_j d_j X_j'$.

Then

$$\begin{pmatrix}\mathbf{X}_1 & \cdots & \mathbf{X}_s\end{pmatrix}\mathbf{h} = h_1\mathbf{X}_1 + \ldots + h_s\mathbf{X}_s = b_1\mathbf{Y}_1 + \ldots + b_w\mathbf{Y}_w = \mathbf{0},$$

where the $\mathbf{Y}_i$ are all of the w distinct monomials appearing on the left-hand side. Note that $b_i = 0$ for all i. Fix such a $\mathbf{Y}_i$ for some $i \in \{1, \ldots, w\}$.

Then

$$b_i\mathbf{Y}_i = \sum_j d_j' X_j' \mathbf{X}_j = \left(\sum_j d_j'\right)\mathbf{Y}_i = \mathbf{0},$$

where the index j ranges over some $J_i \subseteq \{1, \ldots, s\}$ such that $\max(J_i) = t_i$. Every summand above is of the form $d_j' X_j' \mathbf{X}_j = d_j' \mathbf{Y}_i$, where $d_j' X_j'$ is a term in some component of the syzygy $\mathbf{h}$. Note that since we had written the kth syzygy component h_k as a sum of distinct terms, it can contribute at most one term $d'X'$ such that $X'\mathbf{X}_k = \mathbf{Y}_i$ to the sum $b_i\mathbf{Y}_i$. Furthermore, every term $d'X'$ of every syzygy component h occurs in some term $b_{i'}\mathbf{Y}_{i'}$ for $i' \in \{1, \ldots, w\}$.

Return to our previously fixed $i \in \{1, \dots, w\}$. Define a vector $\mathbf{h}^i$ so that its mth component is either $h^i_m = d'_m X'_m$ if h_m contributes to the sum $b_i \mathbf{Y}_i$ or $h^i_m = 0$ otherwise. Then

$$\begin{pmatrix}\mathbf{X}_1 & \cdots & \mathbf{X}_s\end{pmatrix} \mathbf{h}^i = b_i \mathbf{Y}_i = \mathbf{0} \quad \text{and} \quad \mathbf{h} = \sum_{i=1}^{w} \mathbf{h}^i.$$

Using a technique from the proof of Lemma 3.29,

$$\begin{aligned}
\mathbf{h}^i &= \sum_{j \in J_i} d'_j X'_j \mathbf{e}_j = \sum_{j \in J_i} d'_j \frac{\mathbf{Y}_i}{\mathbf{X}_j} \mathbf{e}_j = \\
&= \sum_{j,j' \in J_i \smallsetminus \{t_i\}} \left[\left(\sum_k d' \right) \frac{\mathbf{Y}_i}{\mathbf{X}_{jj'}} \left(\frac{\mathbf{X}_{jj'}}{\mathbf{X}_j} \mathbf{e}_j - \frac{\mathbf{X}_{jj'}}{\mathbf{X}_{j'}} \mathbf{e}_{j'} \right) \right] + \left(\sum_{j \in J_i} d'_j \right) \frac{\mathbf{Y}_i}{\mathbf{X}_{t_i}} \mathbf{e}_{t_i} = \\
&= \sum_{j,j' \in J_i \smallsetminus \{t_i\}} p_{jj'} \mathbf{C}_{jj'},
\end{aligned}$$

so that $\mathbf{h} = \sum_i \mathbf{h}^i = \sum_{j,j'} q_{jj'} \mathbf{C}_{jj'}$ and $\langle C \rangle \supseteq \operatorname{Syz}(\mathbf{X}_1, \dots, \mathbf{X}_s)$, completing the proof. □

We now prove Proposition 4.23.

Proof. We can assume without loss of generality that $\operatorname{LC}(\mathbf{g}_i) = 1$ for all $i \in \{1, \dots, t\}$.

Firstly,

$$\begin{aligned}
\begin{pmatrix}\mathbf{g}_1 & \cdots & \mathbf{g}_t\end{pmatrix} \mathbf{s}_{ij} &= -h_{ij1}\mathbf{g}_1 + \ldots + \left(\frac{\mathbf{X}_{ij}}{\mathbf{X}_i} - h_{iji} \right) \mathbf{g}_i + \ldots + \left(-\frac{\mathbf{X}_{ij}}{\mathbf{X}_j} - h_{ijj} \right) \mathbf{g}_j + \ldots - h_{ijt}\mathbf{g}_t = \\
&= S(\mathbf{g}_i, \mathbf{g}_j) - \sum_{k=1}^{t} h_{ijk} \mathbf{g}_k = \mathbf{0},
\end{aligned}$$

so that $\langle H \rangle \subseteq \operatorname{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_t)$.

Assume, in order to get a contradiction, that $U = \operatorname{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_t) \smallsetminus \langle H \rangle \neq \varnothing$. Select then a $\mathbf{u} \in U$ such that $\mathbf{X} = \max_i (\operatorname{LM}(u_i) \operatorname{LM}(\mathbf{g}_i)) = \max_i (\operatorname{LM}(u_i) \mathbf{X}_i)$ is $<$-minimal by the term order being a well-ordering.

Denote by S the set of indices i such that $\operatorname{LM}(u_i)\mathbf{X}_i = \mathbf{X}$. Define now u'_i for each $i \in \{1, \dots, t\}$ as $u'_i = u_i$ if $i \notin S$ and $u'_i = u_i - \operatorname{LT}(u_i) = u_i - c'_i X'_i$ for $i \in S$. Since $\mathbf{u} \in \operatorname{Syz}(G)$, we necessarily have $\sum_{i \in S} c'_i X'_i \mathbf{X}_i = \mathbf{0}$ so that $\sum_{i \in S} c'_i X'_i \mathbf{e}_i$ is a syzygy of the monomials $\{\mathbf{X}_i \,|\, i \in S\}$. By Lemma 4.24 we can then write

$$\sum_{i \in S} c'_i X'_i \mathbf{e}_i = \sum_{i,j \in S} p_{ij} \left(\frac{\mathbf{X}_{ij}}{\mathbf{X}_i} \mathbf{e}_i - \frac{\mathbf{X}_{ij}}{\mathbf{X}_j} \mathbf{e}_j \right)$$

for some polynomials $p_{ij} \in A$. By observing the left-hand side, we see that every coordinate of the vector contains a single term. We can then choose $p_{ij} = d_{ij} \mathbf{X} / \mathbf{X}_{ij}$ for some constant $d_{ij} \in k$ since $\mathbf{X} = X'_i \mathbf{X}_i$. Rewriting $\mathbf{u}$, we have

$$\begin{aligned}
(u_1, \dots, u_t) &= \sum_{i \in S} c'_i X'_i \mathbf{e}_i + (u'_1, \dots, u'_t) = \sum_{i,j \in S} p_{ij} \left(\frac{\mathbf{X}_{ij}}{\mathbf{X}_i} \mathbf{e}_i - \frac{\mathbf{X}_{ij}}{\mathbf{X}_j} \mathbf{e}_j \right) + (u'_1, \dots, u'_t) = \\
&= \sum_{i,j \in S} p_{ij} \mathbf{s}_{ij} + \sum_{i,j \in S} p_{ij} (h_{ij1}, \dots, h_{ijt}) + (u'_1, \dots, u'_t) = \sum_{i,j \in S} p_{ij} \mathbf{s}_{ij} + (v_1, \dots, v_t).
\end{aligned}$$

By the assumption, $\mathbf{u}, \mathbf{s}_{ij} \in \operatorname{Syz}(G)$ and $\mathbf{u} \notin \langle H \rangle$, so that $\mathbf{v} = (v_1, \dots, v_t) \in \operatorname{Syz}(G) \setminus \langle H \rangle$. We will obtain a contradiction by showing that $\max_k (\operatorname{LM}(v_k)\mathbf{X}_k) < \mathbf{X}$. For each $k \in \{1, \dots, t\}$,

$$\operatorname{LM}(v_k)\mathbf{X}_k = \operatorname{LM}\left(u'_k + \sum_{i,j \in S} p_{ij} h_{ijk} \right) \mathbf{X}_k \leq \max\left(\operatorname{LM}(u'_k), \max_{i,j \in S} \left(\operatorname{LM}(p_{ij}) \operatorname{LM}(h_{ijk}) \right) \right) \mathbf{X}_k.$$

Firstly, $\operatorname{LM}(u'_k)\mathbf{X}_k < \mathbf{X}$ by construction. Secondly, with $p_{ij} = d_{ij}\mathbf{X}/\mathbf{X}_{ij}$ as noted above, we have for $i, j \in S$ that

$$\begin{aligned} \operatorname{LM}(p_{ij}) \operatorname{LM}(h_{ijk})\mathbf{X}_k = \frac{\mathbf{X}}{\mathbf{X}_{ij}} \operatorname{LM}(h_{ijk})\mathbf{X}_k &= \frac{\mathbf{X}}{\mathbf{X}_{ij}} \operatorname{LM}(h_{ijk}) \operatorname{LM}(\mathbf{g}_k) \leq \\ &\leq \frac{\mathbf{X}}{\mathbf{X}_{ij}} \operatorname{LM}(S(\mathbf{g}_i, \mathbf{g}_j)) < \frac{\mathbf{X}}{\mathbf{X}_{ij}} \operatorname{LCM}(\operatorname{LM}(\mathbf{g}_i), \operatorname{LM}(\mathbf{g}_j)) = \mathbf{X}, \end{aligned}$$

so that $\operatorname{LM}(v_k)\mathbf{X}_k < \mathbf{X}$. Hence $\max_k(\operatorname{LM}(v_k)\mathbf{X}_k) < \mathbf{X}$, contradicting the minimality of the choice of $\mathbf{X}$ above. Thus $\langle H \rangle \supseteq \operatorname{Syz}(\mathbf{g}_1, \dots, \mathbf{g}_t)$. □

We now have a tangible way of describing the syzygy module $\operatorname{Syz}(G)$ of a Gröbner basis G by computing the $\mathbf{s}_{ij}$ through reduction of the S-polynomials. One could then imagine computing the *second* syzygy module of G, that is, the relations between the generators of $\operatorname{Syz}(G)$, necessitated in the computations of free resolutions in Section 4.4. To apply the theory above, one would first have to compute a Gröbner basis of $\operatorname{Syz}(G)$ applying Buchberger's algorithm. There is in fact a more refined method which we shall state below. First, we define a technical result that will also be used in the proof of the Hilbert syzygy theorem of Section 4.4.

Proposition 4.25. Given a set of non-zero vectors $G = \{\mathbf{g}_1, \dots, \mathbf{g}_t\} \subseteq A^m$ and a term order $<$ on the monomials of A^m, the following is a term order on A^t:

$$X\mathbf{e}_i \prec Y\mathbf{e}_j \iff \left(\operatorname{LM}(X\mathbf{g}_i) < \operatorname{LM}(Y\mathbf{g}_j)\right) \text{ or } \left(\operatorname{LM}(X\mathbf{g}_i) = \operatorname{LM}(Y\mathbf{g}_j) \text{ and } j < i\right).$$

This is said to be the term order $\prec$ on A^t INDUCED BY G.

Proof. Let $X\mathbf{e}_i$ and $Y\mathbf{e}_j$ be two monomials in A^t. We verify that $\prec$ satisfies the conditions of Definition 4.13.

If $i \neq j$, then since $<$ is a total order,

$$\begin{gathered} \left(\operatorname{LM}(X\mathbf{g}_i) = \operatorname{LM}(Y\mathbf{g}_j) \quad \text{and} \quad (i < j \text{ or } j < i)\right) \quad \text{or} \\ \left(\operatorname{LM}(X\mathbf{g}_i) < \operatorname{LM}(Y\mathbf{g}_j) \quad \text{or} \quad \operatorname{LM}(Y\mathbf{g}_j) < \operatorname{LM}(X\mathbf{g}_i)\right) \end{gathered}$$

so that either $X\mathbf{e}_i \prec Y\mathbf{e}_j$ or $Y\mathbf{e}_j \prec X\mathbf{e}_i$. If $i = j$ and $X \neq Y$, then either $\operatorname{LM}(X\mathbf{g}_i) < \operatorname{LM}(Y\mathbf{g}_i)$ or $\operatorname{LM}(Y\mathbf{g}_i) < \operatorname{LM}(X\mathbf{g}_i)$ since the elements of G are non-zero. Hence $\prec$ is a total order.

Let $Z \in \mathbb{T}^n$ such that $Z \neq 1$. Then $\operatorname{LM}(X\mathbf{g}_i) < Z\operatorname{LM}(X\mathbf{g}_j) = \operatorname{LM}(ZX\mathbf{g}_j)$, so that $X\mathbf{e}_i \prec ZX\mathbf{e}_i$.

Assume now that $X\mathbf{e}_i \prec Y\mathbf{e}_j$ and let $Z \in \mathbb{T}^n$. We wish to show $ZX\mathbf{e}_i \prec ZY\mathbf{e}_j$.

If $\operatorname{LM}(X\mathbf{g}_i) < \operatorname{LM}(Y\mathbf{g}_j)$, then $\operatorname{LM}(ZX\mathbf{g}_i) = Z\operatorname{LM}(X\mathbf{g}_i) < Z\operatorname{LM}(Y\mathbf{g}_j) = \operatorname{LM}(ZY\mathbf{e}_j)$ and $ZX\mathbf{e}_i \prec ZY\mathbf{e}_j$.

Otherwise $\operatorname{LM}(X\mathbf{g}_i) = \operatorname{LM}(Y\mathbf{g}_j)$ and $j < i$, so that $\operatorname{LM}(ZX\mathbf{g}_i) = Z\operatorname{LM}(X\mathbf{g}_i) = Z\operatorname{LM}(Y\mathbf{g}_j) = \operatorname{LM}(ZY\mathbf{g}_i)$ with $j < i$, so that $ZX\mathbf{e}_i \prec ZY\mathbf{e}_j$. □

The following result is due to Schreyer ([CLO05]). For clarity, we will write LM when comparing monomials using the term order on A, $\operatorname{LM}_<$ when comparing using a term order $<$ in A^m and $\operatorname{LM}_\prec$ when using the induced order $\prec$ on the monomials of A^t. We shall return to this notation in later proofs that require paying particular attention to the term orders involved.

Theorem 4.26. (*Schreyer*) Given a Gröbner basis $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\} \subseteq A^m$, the set $H = \{\mathbf{s}_{ij} \mid 1 \leq i < j \leq t\}$ is a Gröbner basis for $\mathrm{Syz}(G)$ with respect to the term order $\prec$ on A^t induced by G.

Proof. Assume that $\mathrm{LC}_<(\mathbf{g}_j) = 1$ for all $j \in \{1, \ldots, t\}$. We first prove that the leading monomial of $\mathbf{s}_{ij}$ with respect to $\prec$ is $\mathrm{LM}_\prec(\mathbf{s}_{ij}) = (\mathbf{X}_{ij}/\mathbf{X}_i)\mathbf{e}_i$ for $1 \leq i < j \leq t$. Firstly,

$$\mathrm{LM}_<\left(\frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{g}_i\right) = \mathrm{LM}_<\left(\frac{\mathbf{X}_{ij}}{\mathbf{X}_j}\mathbf{g}_j\right) = \mathbf{X}_{ij} \quad \text{so that} \quad \frac{\mathbf{X}_{ij}}{\mathbf{X}_j}\mathbf{e}_j \prec \frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{e}_i \quad \text{since} \quad i < j.$$

Consider now a monomial in $(h_{ij1}, \ldots, h_{ijt})$ of the form $X\mathbf{e}_\ell$. Then from the definition of G being a Gröbner basis, $\max_k \big(\mathrm{LM}(h_{ijk})\,\mathrm{LM}_<(\mathbf{g}_k)\big) = \mathrm{LM}_<(S(\mathbf{g}_i, \mathbf{g}_j))$ so that $\mathrm{LM}_<(X\mathbf{g}_\ell) \leq \mathrm{LM}_<(S(\mathbf{g}_i, \mathbf{g}_j))$. Then

$$\mathrm{LM}_<(X\mathbf{g}_\ell) \leq \mathrm{LM}_<(S(\mathbf{g}_i, \mathbf{g}_j)) < \mathbf{X}_{ij} = \mathrm{LM}_<\left(\frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{g}_i\right) \quad \text{and} \quad X\mathbf{e}_\ell \prec \frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{e}_i.$$

Hence $\mathrm{LM}_\prec(\mathbf{s}_{ij}) = (\mathbf{X}_{ij}/\mathbf{X}_i)\mathbf{e}_i$.

Let now $\mathbf{s} \in \mathrm{Syz}(G) \leq A^t$. We wish to show that H satisfies condition 1 of Theorem 4.20, i.e. that there exist $i, j \in \{1, \ldots, t\}$ such that $\mathrm{LM}_\prec(\mathbf{s}_{ij})$ divides $\mathrm{LM}_\prec(\mathbf{s})$.

Write $\mathbf{s} = \sum_k p_k \mathbf{e}_k$ for polynomials $p_k \in A$ and let $\mathrm{LT}(p_k) = c_k Y_k$. Then for the leading monomial of $\mathbf{s}$ with respect to $\prec$, we have $\mathrm{LM}_\prec(\mathbf{s}) = Y_i \mathbf{e}_i$ for an $i \in \{1, \ldots, t\}$. Fix this i and let $S_i \subseteq \{1, \ldots, t\}$ be the set of indices k such that $\mathrm{LM}_<(Y_k \mathbf{g}_k) = \mathrm{LM}_<(Y_i \mathbf{g}_i)$. Then for all $k \in S_i$, $k \geq i$ from the definition of $\prec$.

Since $\mathbf{s}$ is a syzygy of G, we have $\begin{pmatrix}\mathbf{g}_1 & \cdots & \mathbf{g}_t\end{pmatrix}\mathbf{s} = \mathbf{0}$ and the coefficient of every term on the left-hand side is 0. In particular, the coefficient of $\mathrm{LM}_<(Y_i \mathbf{g}_i)$ is 0, so that the construction $\mathbf{s}' = \sum_{k \in S_i} c_k Y_k \mathbf{e}_k$ is a syzygy of $\mathrm{LT}_<(\mathbf{g}_1), \ldots, \mathrm{LT}_<(\mathbf{g}_t)$, that is, $\begin{pmatrix}\mathrm{LT}_<(\mathbf{g}_1) & \cdots & \mathrm{LT}_<(\mathbf{g}_t)\end{pmatrix}\mathbf{s}' = \mathbf{0}$.

Then by Lemma 4.24, the syzygy $\mathbf{s}'$ is in the module generated by C so that

$$\mathbf{s}' = \sum_{k, k' \in S_i} p_{kk'} \left(\frac{\mathbf{X}_{kk'}}{\mathbf{X}_k}\mathbf{e}_k - \frac{\mathbf{X}_{kk'}}{\mathbf{X}_{k'}}\mathbf{e}_{k'}\right)$$

for polynomials $p_{kk'} \in A$. Since $\mathrm{LM}_\prec(\mathbf{s}') = \mathrm{LM}_\prec(\mathbf{s}) = Y_i \mathbf{e}_i$ and $k > i$ for $k \in S_i \setminus \{i\}$, we have that

$$c_i Y_i \mathbf{e}_i = \mathrm{LT}_\prec(\mathbf{s}') = \sum_{\substack{k \in S_i \setminus \{i\} \\ \mathrm{LM}(p_{ik}) X_{ik}/X_k = Y_i}} \mathrm{LT}(p_{ik}) \frac{X_{ik}}{X_i} \mathbf{e}_i,$$

so that there exists an index $j \in S_i \setminus \{i\}$ such that $(X_{ij}/X_i)\mathbf{e}_i = \mathrm{LM}_\prec(\mathbf{s}_{ij})$ divides the leading term of the syzygy $\mathrm{LM}_\prec(\mathbf{s}') = \mathrm{LM}_\prec(\mathbf{s}')$. Hence H is a Gröbner basis of $\mathrm{Syz}(G)$. □

We now move on to some computations in module theory that will make use of the above results.

4.4. Free resolutions and the Hilbert syzygy theorem

For the rest of the text, we will be dealing with sequences of module homomorphisms. We introduce the common compact way of writing down such information in homological algebra:

Definition 4.27. Let M^i be A-modules. A (possibly infinite) sequence $M^\bullet$ of A-module homomorphisms ϕ_i

$$M^0 \xrightarrow{\phi_0} M^1 \xrightarrow{\phi_1} \cdots \xrightarrow{\phi_{i-1}} M^i \xrightarrow{\phi_i} \cdots \xrightarrow{\phi_{n-1}} M^n$$

is said to be EXACT AT POSITION i if $\operatorname{im}\phi_{i-1} = \ker\phi_i$. If $M^\bullet$ is exact at all $i \in \{1, \dots, n-1\}$, it is said to be an EXACT SEQUENCE.

Example 4.28. The statement that the sequence

$$0 \longrightarrow M \xrightarrow{\phi} M'$$

is exact is equivalent to stating that $\phi : M \to M'$ is injective, since exactness means $\operatorname{im} 0 = 0 = \ker\phi$. Similarly, $\psi : M \to M'$ is surjective if and only if the sequence

$$M \xrightarrow{\psi} M' \longrightarrow 0$$

is exact since exactness means $\operatorname{im}\psi = \ker 0 = M'$. △

Recall from Lemma 4.9 that an arbitrary finitely generated A-module M taken as the image of a homomorphism ϕ_0 has a *presentation*, i.e. we have $M \cong A^{s_0}/M_0$ for a $s_0 \in \mathbb{N}$ and some submodule $M_0 \leq A^{s_0}$, the kernel of ϕ_0, i.e. the syzygy module of the generators of M. This corresponds to the exact sequence

$$0 \to M_0 \xrightarrow{\iota_0} A^{s_0} \xrightarrow{\phi_0} M \to 0,$$

where ι_0 is the inclusion map. We can then find an analogous presentation for M_0 as a quotient of some free module A^{s_1} with some submodule M_1 (the second-order syzygy module, i.e. the relations between the generators of the first syzygy module), etc. Repeating this process we obtain a succession of presentations of modules and composing appropriate homomorphisms we can construct the following diagram:

$$\begin{tikzcd}
 & & 0 \arrow[dr] & & 0 & & & & \\
 & & & M_1 \arrow[ur] \arrow[dr] & & & & & \\
\cdots \arrow[rr] \arrow[dr] & & A^{s_2} \arrow[rr] \arrow[ur] & & A^{s_1} \arrow[rr] \arrow[dr] & & A^{s_0} \arrow[r] & M \arrow[r] & 0. \\
 & M_2 \arrow[ur] \arrow[dr] & & & & M_0 \arrow[ur] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

Taking the horizontal sequence of maps, we see that we have in a sense decomposed (*resolved*) M by the free modules A^{s_i}.

Definition 4.29. An exact sequence $M^\bullet$ of the form

$$\cdots \longrightarrow A^{s_2} \longrightarrow A^{s_1} \longrightarrow A^{s_0} \longrightarrow M \longrightarrow 0$$

for an A-module M and free A-modules A^{s_i} is said to be a FREE RESOLUTION of M. If furthermore $M^\bullet$ is finite and for all $i \geq n$, $A^{s_i} = 0$, it is said to be of FINITE LENGTH n.

Example 4.30. Consider Example 4.11 for $n = 2$ with $A = k[x, y]$. By Lemma 4.24 we can see that the first syzygy module is given by

$$\operatorname{Syz}(\ker\phi) = \operatorname{Syz}(x, y) = \left\langle \frac{xy}{x}\mathbf{e}_1 - \frac{xy}{y}\mathbf{e}_2 \right\rangle = \langle (y, -x) \rangle.$$

This can be reached by a homomorphism of A_1 and its kernel, the second syzygy module $\mathrm{Syz}((y,-x))$, is trivial. Thus the following finite free resolution is obtained:

$$0 \longrightarrow A^1 \xrightarrow{F_1} A^2 \xrightarrow{F_2} A^1 \xrightarrow{\phi} k \longrightarrow 0$$

with the maps given by

$$F_1 = \begin{pmatrix} -y \\ x \end{pmatrix}, \qquad F_2 = \begin{pmatrix} x & y \end{pmatrix}.$$

$\triangle$

Example 4.31. Consider Example 4.11 with $n = 3$. We obtain the resolution

$$0 \longrightarrow A^1 \xrightarrow{F_1} A^3 \xrightarrow{F_2} A^3 \xrightarrow{F_3} A^1 \xrightarrow{\phi} k \longrightarrow 0$$

where the maps are given by

$$F_1 = \begin{pmatrix} z \\ -y \\ x \end{pmatrix}, \qquad F_2 = \begin{pmatrix} -y & -z & 0 \\ x & 0 & -z \\ 0 & x & y \end{pmatrix}, \qquad F_3 = \begin{pmatrix} x & y & z \end{pmatrix}.$$

$\triangle$

Example 4.32. In a similar vein, consider the ideal of symmetric polynomials, $\langle \sigma_1, \sigma_2, \sigma_3 \rangle$ in $A = k[x, y, z]$ as defined in 3.5. We obtain a free resolution of the form

$$0 \longrightarrow A^1 \stackrel{B_1}{\longrightarrow} A^3 \stackrel{B_2}{\longrightarrow} A^3 \longrightarrow \langle \sigma_1, \sigma_2, \sigma_3 \rangle \longrightarrow 0.$$

with

$$B_1 = \begin{pmatrix} z^3 \\ -y^2 - yz - z^2 \\ x + y + z \end{pmatrix}, \qquad B_2 = \begin{pmatrix} 0 & x + y + z & y^2 + yz + z^2 \\ -x - y - z & -xz - yz - z^2 & -y^2 z - yz^2 \\ xy + xz + yz & xz^2 + yz^2 & y^2 z^2 \end{pmatrix}.$$

Disregarding the sign of the middle row, the 1-by-3 matrix B_1 contains exactly the Gröbner basis for the ideal as presented in 3.5. $\triangle$

Remark. The curious reader will probably notice from the examples above that the dimensions of the free modules in the resolution of k for the polynomial ring of n variables bear resemblance to the $(n + 1)$th row of Pascal's triangle. Indeed, this is not a coincidence but rather a consequence of deeper results on Hilbert functions, Betti numbers and Euler characteristics. Further exposition is beyond the scope of this text and can be found in, for example, [Eis05].

For the example with symmetric polynomials, the observation is related to the algebraic independence of the polynomials and the fundamental theorem of symmetric polynomials 3.41. Again, this topic is beyond the scope of this text. A detailed presentation can be found in [CLO07].

We now stand ready to formulate a fundamental result in commutative algebra. Using the Gröbner basis machinery developed in this section we will be able to give a constructive proof of this result for the case of A-modules.

Theorem 4.33. (*Hilbert syzygy theorem*) *Every finitely generated A-module has a free resolution of length $\leq n$.*

Remark. Free resolutions of A-modules are not unique, nor are the dimensions of the free modules involved. One invariant however is the alternating sum of these dimensions (this is formulated using the theory of Hilbert functions in, for instance, [CLO05]). The proof of the Hilbert syzygy theorem will nevertheless yield a constructive method of computing a resolution of length $\leq n$. This length is termed the *global dimension* of A, a homological invariant of the polynomial ring itself.

In order to prove Theorem 4.33, we will require the following technical result making use of the term order $\prec$ described in Proposition 4.25. We will once again use the notation for leading monomials defined before Theorem 4.26.

Lemma 4.34. Let $G = \{\mathbf{g}_1 \dots, \mathbf{g}_t\}$ be the Gröbner basis of a submodule of A^m with respect to a term order $<$. Arrange the elements of G so that whenever the leading terms $\mathrm{LT}_<(\mathbf{g}_i) = cX\mathbf{e}_k$ and $\mathrm{LT}_<(\mathbf{g}_j) = dY\mathbf{e}_\ell$ have the same basis vector, i.e. if $k = \ell$ and $i < j$, then $X >_{\mathrm{lex}} Y$ with respect to the lex order on A with $x_1 > \cdots > x_n$. Then the following holds:

1. If the variables $x_1, \dots, x_m$ for $m \in \{1, \dots, n-1\}$ do not appear in some $\mathrm{LM}_<(\mathbf{g}_j)$ for $j \in \{1, \dots, t\}$, then the variables $x_1, \dots, x_{m+1}$ do not appear in $\mathrm{LM}_\prec(\mathbf{s}_{jz})$ for $z \in \{j+1, \dots, t\}$. Consequently, if $x_1, \dots, x_m$ do not appear in any $\mathrm{LM}_<(\mathbf{g}_j)$, then $x_1, \dots, x_{m+1}$ do not appear in any $\mathrm{LM}_\prec(\mathbf{s}_{jz})$ for $1 \leq j < z \leq t$.
2. x_1 does not appear in any $\mathrm{LM}_\prec(\mathbf{s}_{jz})$ for $1 \leq j < z \leq t$.

Proof. Let $i, j \in \{1, \dots, t\}$ such that $i < j$. If $\mathrm{LM}_<(\mathbf{g}_i)$ and $\mathrm{LM}_<(\mathbf{g}_j)$ have different basis vectors, then $\mathbf{X}_{ij} = \mathbf{s}_{ij} = \mathbf{0}$ so that no variables appear in $\mathbf{s}_{ij}$. Assume thus that $\mathrm{LM}_<(\mathbf{g}_i) = X_i\mathbf{e}_\ell$ and $\mathrm{LM}_<(\mathbf{g}_j) = X_j\mathbf{e}_\ell$ for some $\ell \in \{1, \dots, m\}$.

From the first part of the proof of Theorem 4.26, we have $\mathrm{LM}_\prec(\mathbf{s}_{ij}) = (\mathbf{X}_{ij}/\mathbf{X}_i)\mathbf{e}_i = (X_{ij}/X_i)\mathbf{e}_i$. Assume now that $x_1, \dots, x_m$ do not appear in X_i. Since $i < j$, we have $X_i >_{\mathrm{lex}} X_j$ by the arrangement of the elements of G, so that the variables $x_1, \dots, x_m$ do not appear in X_j and the power of x_{m+1} in X_i is equal to or larger than the power of x_{m+1} in X_j by Definition 3.8. Then the power of x_{m+1} in X_{ij} is the largest of these two powers and hence $x_1, \dots, x_{m+1}$ do not appear in X_{ij}/X_i, nor in $(\mathbf{X}_{ij}/\mathbf{X}_i)\mathbf{e}_i = \mathrm{LM}_\prec(\mathbf{s}_{ij})$.

Thus if the variables $x_1, \dots, x_m$ do not appear in any $\mathrm{LM}_<(\mathbf{g}_i)$ for $i \in \{1, \dots, s\}$, the variables $x_1, \dots, x_{m+1}$ do not appear in any $\mathrm{LM}_\prec(\mathbf{s}_{ij})$ for $1 \leq i < j \leq t$.

We now wish to show the last statement. Since $i < j$, we have that $X_i >_{\mathrm{lex}} X_j$, so that the power of x_1 in X_i is equal to or larger than the power of x_1 in X_j. Then the power of x_1 appearing in X_{ij} is the largest of these two powers, so that x_1 does not appear in $\mathrm{LM}_\prec(\mathbf{s}_{ij})$. □

We now give the proof of Theorem 4.33:

Proof. Let $M \cong A^{s_0}/M_0$ be a presentation of the (finitely generated) A-module M. If $M_0 = \{\mathbf{0}\}$, the resolution is trivial. Otherwise, a Gröbner basis of M_0 exists with respect to some term order $<$ on the monomials of A^{s_0} so we can write $M_0 = \langle G \rangle = \langle \mathbf{g}_1, \dots, \mathbf{g}_t \rangle$, letting said Gröbner basis be the generating set of M_0. Arranging the elements of G according to Lemma 4.34, let $i \in \{0, \dots, n\}$ be such that $x_1, \dots, x_i$ do not appear in any $\mathrm{LM}_<(\mathbf{g}_j)$ for $j \in \{1, \dots, t\}$. Then either $i = n$ or $i < n$.

If $i = n$, none of the variables appear in any $\mathrm{LM}_<(\mathbf{g}_j)$. Then $\mathrm{LT}_<(\mathbf{g}_j) = a\mathbf{e}_\ell$ for some coefficient $a \in k$ and $\ell \in \{1, \dots, s_0\}$ so that the leading term module $\mathrm{LT}_<(G)$ is generated by the basis vectors $\mathbf{e}_\ell$ appearing in the leading terms of the elements of G and is thus free. Let M' be the free module generated by the basis vectors that do not generate $\mathrm{LT}_<(G)$ and construct the homomorphism

$$\begin{array}{rccccc} \pi : & M' & \to & A^{s_0}/M_0 & \cong & M \\ & \mathbf{f} & \mapsto & \mathbf{f} + M_0. & & \end{array}$$

We wish to show that π is a bijection. Let $\mathbf{f}$ be such that $\mathbf{f} \in M_0$ and $\mathbf{f} \in M'$, so that $\mathbf{f} \in \ker \pi$. Then $\mathrm{LM}_<(\mathbf{f})$ is divisible by some $\mathrm{LM}_<(\mathbf{g}_j)$ since G is a Gröbner basis of M_0. Since $\mathbf{f} \in M'$, it consists of terms that do not feature the basis vectors appearing in the leading terms of the $\mathbf{g}_j$ so that $\mathbf{f} = \mathbf{0}$, $\ker \pi = \{\mathbf{0}\}$ and π is injective.

For all $\mathbf{f} \in A^{s_0}$, we have that $\mathbf{f}$ reduces as $\mathbf{f} \xrightarrow{G}_+ \mathbf{r}$ by G for a unique remainder $\mathbf{r}$ (again since G is a Gröbner basis of M_0), so that $\mathbf{f} - \mathbf{r} \in M_0$ and $\mathbf{f} + M_0 = \mathbf{r} + M_0$. Since $\mathbf{r}$ is reduced with respect to G, no term in $\mathbf{r}$ is divisible by any $\mathrm{LM}_<(\mathbf{g}_j)$, that is, $\mathbf{r}$ does not contain the basis vectors which appear in the leading monomials $\mathrm{LM}_<(\mathbf{g}_j)$. Hence $\mathbf{r} \in M'$ and π is surjective. By the isomorphism theorem, $M' \cong A^{s_0}/M_0 \cong M$ and M is free, terminating the exact sequence.

If $i < n$, construct the jth step of the following free resolution

$$A^{s_j} \xrightarrow{\phi_j} A^{s_{j-1}} \xrightarrow{\phi_{j-1}} \cdots \xrightarrow{\phi_2} A^{s_1} \xrightarrow{\phi_1} A^{s_0} \xrightarrow{\phi_0} M \longrightarrow 0$$

as follows:

Let $<$ be a monomial order on A^{s_j} and let G_j be a Gröbner basis of $\ker \phi_j \leq A^{s_j}$. Arrange the elements of G_j according to Lemma 4.34 and let s_{j+1} be the number of basis elements $s_{j+1} = |G_j|$. Construct ϕ_{j+1} as the customary projective homomorphism from the free module $A^{s_{j+1}}$ onto $\ker \phi_j$.

By Lemma 4.34 and the assumption that the variables $x_1, \ldots, x_i$ do not appear in the leading monomials of the elements of the Gröbner basis of M_0, i.e. the $\mathrm{LM}_<(\mathbf{g}_j)$, we have that $x_1, \ldots, x_{i+1}$ do not appear in the leading monomials $\mathrm{LM}_\prec(\mathbf{s}_{ij})$ of the Gröbner basis of $\mathrm{Syz}(G)$ with respect to the term order $\prec$ induced by G. Furthermore, regardless if x_1 appears or does not appear in some $\mathrm{LM}_<(\mathbf{g}_j)$, then x_1 does not appear in any leading monomial of the Gröbner basis of $\mathrm{Syz}(G)$.

Hence we can apply Lemma 4.34 repeatedly so that no variables appear in the leading monomials of the generators of $\ker \phi_{n-i}$, reducing the resolution of $\ker \phi_{n-i}$ to the case above, yielding that

$$A^{s_{n-i}} / \ker \phi_{n-i} \cong \operatorname{im} \phi_{n-i}$$

is a free module. Then replacing $A^{s_{n-i}}$ with $A^{s_{n-i}}/\ker \phi_{n-i}$ at index $n - i$ in the sequence terminates the resolution. □

Remark. Computing the free resolution of an A-module M by applying Lemma 4.34 and using the induced Schreyer orders $\prec$ at every step as in the proof of Theorem 4.33, one algorithmically arrives at a sequence of length $\leq n$. However, this process is computationally very cumbersome since a comparison of two terms at the ith step using $\prec_i$ recursively requires the previous $i-1$ term orders and Gröbner bases for comparisons in the free modules above. This algrotihmically naïve approach is therefore typically avoided as there exist refined, substantially more efficient algorithms which, for instance, omit terms in the module elements which are not used during computation and utilise deeper theory such as that of Schreyer frames. The details of such implementations are beyond the scope of this text. An example of current research in the field can be found in [EMSS15].

Example 4.35. (Exercise 3.10.1 in Adams & Loustaunau, [AL94]*)* We calculate a free resolution for the module generated by

$$(x, y, z), (y, x, z), (y, z, x), (x, z, y), (y, x - z, z), (y, z, x - z) \in \mathbb{Q}[x, y, z]^3$$

for the lex term order with TOP.

Implementing the above algorithms in `sagemath`,we find a free resolution:

$$0 \longrightarrow A^1 \xrightarrow{B_1} A^4 \xrightarrow{B_2} A^6 \longrightarrow M \longrightarrow 0$$

We verify this calculation with `macaulay2`.The intermediate maps $B_1 : A^1 \to A^4$ and $B_2 : A^4 \to A^6$ are given by the matrices

$$B_1 = \begin{pmatrix} -z \\ -y+z \\ x-z \\ 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} -x+z & 0 & -z & -yz-z^2 \\ y-z & x-2z & y-z & -x^2+y^2+yz+z^2 \\ -y+z & -x+2z & -y+z & -z^2 \\ x-z & 0 & z & z^2 \\ 0 & -x+z & -y+z & x^2+xz-y^2-yz \\ 0 & x-z & y-z & 0 \end{pmatrix}.$$

It is readily verified that $B_2B_1 = 0$ so that $\operatorname{im} B_1 \subseteq \ker B_2$. For the other inclusion, using the methods outlined in sections 4.2 and 4.3 we can compute the syzygy module of the columns of B_2, i.e. $\ker B_2$ and see that its generator is the column vector of B_1. Thus $\operatorname{im} B_1 = \ker B_2$. △

Example 4.36. (Example from page 253 of Cox, Little & O'Shea, [CLO05]*)* We calculate a free resolution for the ideal

$$M = \langle yz - xw, y^3 - x^2z, xz^2 - y^2w, z^3 - yw^2 \rangle \trianglelefteq k[x, y, z, w] = A$$

with degrevlex.

Calculations with `macaulay2` as described above give the following free resolution:

$$0 \longrightarrow A^1 \xrightarrow{B_1} A^4 \xrightarrow{B_2} A^4 \longrightarrow M \longrightarrow 0$$

The intermediate maps are given by:

$$B_1 = \begin{pmatrix} w \\ -z \\ -y \\ x \end{pmatrix}, \quad B_2 = \begin{pmatrix} -y^2 & -xz & -yw & -z^2 \\ z & w & 0 & 0 \\ x & y & -z & -w \\ 0 & 0 & x & y \end{pmatrix}.$$

△

4.5. The Hom module

We are now interested in the explicit computation of two particular objects in the setting of A-modules. The first one, Hom, is presented here. The other is covered in 4.7. These objects from homological algebra cannot be given a proper theoretical treatment in this text. Such an exposition can be found in [Wei94].

Definition 4.37. Let M, N be A-modules. Then we define $\operatorname{Hom}(M, N)$ to be the set of A-module homomorphisms $\phi : M \to N$. $\operatorname{Hom}(M, N)$ is in particular an A-module under addition of homomorphisms $(\phi + \psi)(\mathbf{m}) = \phi(\mathbf{m}) + \psi(\mathbf{m})$ and the following multiplication by elements $a \in A$:

$$(a\phi)(\mathbf{m}) = a(\phi(\mathbf{m})) = \phi(a\mathbf{m}).$$

For two free A-modules A^s, A^t we can associate the matrix of a homomorphism $\phi : A^s \to A^t$ with the vector in A^{st} consisting of the concatenated columns of the matrix ϕ such that $\mathrm{Hom}(A^s, A^t) \cong A^{st}$. This will enable us to use explicit methods in 4.6.

The following result from homological algebra is useful:

Proposition 4.38. Given A-modules M_i, P and A-module homomorphisms ϕ, ψ satisfying the exact sequence

$$M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \longrightarrow 0$$

the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(M_3, P) \xrightarrow{\circ\psi} \mathrm{Hom}(M_2, P) \xrightarrow{\circ\phi} \mathrm{Hom}(M_1, P)$$

If the module P is free, the following sequence is also exact:

$$\mathrm{Hom}(P, M_1) \xrightarrow{\phi_\circ} \mathrm{Hom}(P, M_2) \xrightarrow{\psi_\circ} \mathrm{Hom}(P, M_3) \longrightarrow 0$$

Remark. These properties can be referred to by saying that Hom is a left-exact functor. Furthermore, the only statement in the second sequence that requires P to be free is that $\psi_\circ$ is surjective – this statement is in fact equivalent to the definition of P being a projective module. The Quillen-Suslin theorem states that every finitely generated projective module over a polynomial ring is a free module, so in our scenario we will not discuss projective modules further. We refer to [Lan02] for details on these properties and a proof of the mentioned theorem.

Proof. See [AL94]. □

By Lemma 4.9, we have $M \cong A^s/L$ and $N \cong A^t/K$ for some $s, t \in \mathbb{N}$, $L \leq A^s$ and $K \leq A^t$. Taking one step in the free resolutions of M and N, respectively, we have the exact sequences

$$A^{s_1} \xrightarrow{\Gamma} A^s \xrightarrow{\pi} M \longrightarrow 0 \quad \text{and} \quad A^{t_1} \xrightarrow{\Delta} A^t \xrightarrow{\pi'} N \longrightarrow 0\ ,$$

where Γ and Δ are projections of the basis vectors of their respective domains onto the generating sets of L and K and π and π' are the ordinary projections of basis vectors onto the generating sets of M and N.

Using Proposition 4.38 we thus obtain three exact sequences:

$$0 \longrightarrow \mathrm{Hom}(M, N) \xrightarrow{\circ\pi} \mathrm{Hom}(A^s, N) \xrightarrow{\circ\Gamma} \mathrm{Hom}(A^{s_1}, N)$$

$$\mathrm{Hom}(A^s, A^{t_1}) \xrightarrow{\Delta_\circ} \mathrm{Hom}(A^s, A^t) \xrightarrow{\pi'_\circ} \mathrm{Hom}(A^s, N) \longrightarrow 0$$

$$\mathrm{Hom}(A^{s_1}, A^{t_1}) \xrightarrow{\Delta_\circ} \mathrm{Hom}(A^{s_1}, A^t) \xrightarrow{\pi'_\circ} \mathrm{Hom}(A^{s_1}, N) \longrightarrow 0.$$

Since composition with Γ also gives rise to a homomorphism $\mathrm{Hom}(A^s, A^t) \to \mathrm{Hom}(A^{s_1}, A^t)$ and since $(\pi' \circ f) \circ \Gamma = \pi' \circ (f \circ \Gamma)$, we can arrange the sequences in the following commutative diagram with the diagonal map $\varphi = {}_\circ\Gamma \circ \pi'_\circ$:

$$\begin{tikzcd}
 & & 0 & 0 \\
0 \arrow[r] & \mathrm{Hom}(M,N) \arrow[r, "{}_\circ\pi"] & \mathrm{Hom}(A^s,N) \arrow[u] \arrow[r, "{}_\circ\Gamma"] & \mathrm{Hom}(A^{s_1},N) \arrow[u] \\
 & & \mathrm{Hom}(A^s,A^t) \arrow[u, "{\pi'}_\circ"] \arrow[r, "{}_\circ\Gamma"] \arrow[ur, "\varphi"] & \mathrm{Hom}(A^{s_1},A^t) \arrow[u, "{\pi'}_\circ"] \\
 & & \mathrm{Hom}(A^s,A^{t_1}) \arrow[u, "\Delta_\circ"] & \mathrm{Hom}(A^{s_1},A^{t_1}) \arrow[u, "\Delta_\circ"]
\end{tikzcd}$$

Denote the kernel of ${}_\circ\Gamma$ in $\mathrm{Hom}(A^s, N)$ by K. From the isomorphism theorem for modules, it can be identified that:

$$\begin{aligned}
\mathrm{Hom}(M,N) &\cong K \\
\mathrm{Hom}(A^s,N) &\cong \mathrm{Hom}(A^s,A^t)/\operatorname{im}(\Delta_\circ) \\
\mathrm{Hom}(A^{s_1},N) &\cong \mathrm{Hom}(A^{s_1},A^t)/\operatorname{im}(\Delta_\circ)
\end{aligned}$$

From the exactness it is seen that $\pi'_\circ$ is surjective and therefore K is exactly the image of $\ker\varphi$ under $\pi'_\circ$. The isomorphism theorem again gives that $K \cong \ker\varphi/\ker\pi'_\circ = \ker\varphi/\operatorname{im}\Delta_\circ$, and thus $\mathrm{Hom}(M,N) \cong \ker\varphi/\operatorname{im}\Delta_\circ$. This is a quotient of two submodules of Hom modules, isomorphic to two submodules of two free A-modules (since $\mathrm{Hom}(A^i, A^j) \cong A^{ij}$, as discussed above) and can as such be computed in a straightforward way, as we shall see in the following section.

4.6. Explicit calculation of Hom

To make use of Gröbner methods, we will now follow the theory of the previous section with explicit methods and calculations of the associated matrices. This section roughly follows the reasoning sketched in [AL94], filling in the omitted details in the reasoning and correcting some minor inconsistencies.

The lemmas of this section deal with the associated matrices of maps discussed in Section 4.5. The proofs of these results are technical and will be omitted. The interested reader can find these in [AL94].

Lemma 4.39. For a map $\rho : A^{\ell t_1} \to A^{\ell t}$ associated with S_ℓ, as above for $\rho = \delta$ and $\ell = s$, we have that

$$S_\ell = \bigoplus_{i=1}^{\ell} \Delta,$$

where $\oplus$ denotes the block sum of matrices obtained by concatenation along the diagonal.

Hence we have, with $\langle T \rangle$ denoting the submodule generated by the column vectors of a matrix $T \in A^{x\times y}$,

$$\begin{aligned}
\mathrm{Hom}(A^s,N) &\cong \mathrm{Hom}(A^s,A^t)/\operatorname{im}(\Delta_\circ) \cong A^{st}/\langle S_s\rangle \\
\mathrm{Hom}(A^{s_1},N) &\cong \mathrm{Hom}(A^{s_1},A^t)/\operatorname{im}(\Delta_\circ) \cong A^{s_1 t}/\langle S_{s_1}\rangle.
\end{aligned}$$

Then the map ${}_\circ\Gamma : \mathrm{Hom}(A^s, N) \to \mathrm{Hom}(A^{s_1}, N)$ induces a map $\gamma : A^{st}/\langle S_s\rangle \to A^{s_1 t}/\langle S_{s_1}\rangle$ and we have the following result:

Proposition 4.40. The map γ above is defined by

$$\begin{array}{rccc} \gamma: & A^{st}/\langle S_s\rangle & \to & A^{s_1t}/\langle S_{s_1}\rangle \\ & \mathbf{m}+\langle S_s\rangle & \mapsto & T\mathbf{m}+\langle S_{s_1}\rangle, \end{array}$$

where

$$T = {}^t(\Gamma\otimes I_t)\in A^{s_1t\times st},$$

I_t denotes the identity matrix of $A^{t\times t}$ and $\otimes$ denotes the tensor product, i.e. replacing the i,jth element γ_{ij} of Γ by $\gamma_{ij}I_t$.

We now state a result on presentations of quotient modules.

Proposition 4.41. Given submodules $M,N\leq A^m$ such that $N\subset M$, $M=\langle \mathbf{f}_1,\dots,\mathbf{f}_s\rangle$ and $N=\langle \mathbf{g}_1,\dots,\mathbf{g}_t\rangle$, define the following A-module homomorphism:

$$\begin{array}{rccl} \phi: & A^s & \to & M/N \\ & \mathbf{e}_i & \mapsto & \mathbf{f}_i+N \quad i\in\{1,\dots,s\}. \end{array}$$

Let furthermore $H=\begin{pmatrix}\mathbf{f}_1 & \cdots & \mathbf{f}_s & \mathbf{g}_1 & \cdots & \mathbf{g}_t\end{pmatrix}\in A^{m\times(s+t)}$ and $\mathrm{Syz}(H)=\langle \mathbf{p}_1,\dots,\mathbf{p}_r\rangle\leq A^{s+t}$. Denoting by $\mathbf{h}_i\in A^s$ the vector containing the first s coordinates of $\mathbf{p}_i$ for $i\in\{1,\dots,r\}$, we have that

$$\ker\phi=\langle \mathbf{h}_1,\dots,\mathbf{h}_r\rangle.$$

Proof. See [AL94]. □

Construct the homomorphism in Proposition 4.41 for our scenario:

$$\begin{array}{rccc} \gamma': & A^{st} & \to & A^{s_1t}/\langle S_{s_1}\rangle \\ & \mathbf{m} & \mapsto & T\mathbf{m}+\langle S_{s_1}\rangle, \end{array}$$

where T is the matrix from the definition of γ and $U=\begin{pmatrix}\mathbf{u}_1 & \cdots & \mathbf{u}_u\end{pmatrix}\in A^{st\times u}$ for some $u\in\mathbb{N}$ is the matrix such that $\langle U\rangle=\ker(\gamma')\leq A^{st}$. Thus $\gamma'=\pi\circ T$, summarized in the diagrams below:

$$\begin{tikzcd} A^{st} \arrow[r, "T"] \arrow[d, "\pi"] \arrow[dr, "\gamma'"] & A^{s_1t} \arrow[d, "\pi"] \\ A^{st}/\langle S_s\rangle \arrow[r, "\gamma"'] & A^{s_1t}/\langle S_{s_1}\rangle \end{tikzcd} \qquad \begin{tikzcd} \mathbf{m} \arrow[r, mapsto, "T"] \arrow[d, mapsto, "\pi"] \arrow[dr, mapsto, "\gamma'"] & T\mathbf{m} \arrow[d, mapsto, "\pi"] \\ \mathbf{m}+\langle S_s\rangle \arrow[r, mapsto, "\gamma"'] & T\mathbf{m}+\langle S_{s_1}\rangle. \end{tikzcd}$$

Thus by our previous results

$$\mathrm{Hom}(M,N)\cong\ker{}_\circ\Gamma\cong\ker\gamma\cong\ker\gamma'/\langle S_s\rangle\cong\langle U\rangle/\langle S_s\rangle.$$

Applying Proposition 4.41 again construct a homomorphism

$$\begin{array}{rccl} \xi: & A^u & \to & \langle U\rangle/\langle S_s\rangle \\ & \mathbf{e}_i & \mapsto & \mathbf{u}_i+\langle S_s\rangle \quad i\in\{1,\dots,u\}, \end{array}$$

so that

$$\mathrm{Hom}(M,N)\cong\langle U\rangle/\langle S_s\rangle\cong A^u/\ker\xi,$$

where $\ker\xi$ is obtained as described in Proposition 4.41. This is the desired presentation of $\mathrm{Hom}(M,N)$. We summarize the steps of our computation below.

Summary 4.42. Let $M\cong A^s/L$ and $N\cong A^t/K$ be A-modules. Then, with the notation used above, $\mathrm{Hom}(M,N)$ is computed as follows:

1. Construct the matrices Γ and Δ from the generating sets of L and K, respectively.
2. Compute $T = {}^t(\Gamma \otimes I_t)$.
3. Compute the matrix U as $\ker \gamma'$ using the theorem above.
4. Compute $\ker \xi$. We now have a presentation of $\operatorname{Hom}(M, N)$ as $A^u / \ker \xi$.

Example 4.43. We now show calculations of Hom between two modules as indicated in example 3.9.6 of [AL94] using the degrevlex order, following the procedure of Summary 4.42.

Consider the module M generated by the columns of the matrix

$$F = \begin{pmatrix} xy & y & 0 & yz \\ xz & x & x^3 - x^2 z & x^2 \\ yz & y & x^2 y - xyz & xy \end{pmatrix}$$

and the module N generated by the columns of

$$G = \begin{pmatrix} x^2 & x^2 & x^2 z \\ y^2 & yz & xy^2 + yz^2 \end{pmatrix}.$$

We calculate the first maps of their respective free resolutions to

$$\Delta = \begin{pmatrix} xy \\ -xy + yz - z^2 \\ -y + z \end{pmatrix}, \qquad \Gamma = \begin{pmatrix} -1 & -z & -xz \\ x + z & z^2 & 0 \\ 0 & -1 & -x - z \\ -1 & x - z & x^2 \end{pmatrix}.$$

The values of the constants s, s_1, t, t_1 are thus $4, 3, 3, 1$.

The tensor product $T = {}^t(\Gamma \otimes I_t)$ is easily written as

$$\begin{pmatrix} -1 & 0 & 0 & x+z & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & x+z & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & x+z & 0 & 0 & 0 & 0 & 0 & -1 \\ -z & 0 & 0 & z^2 & 0 & 0 & -1 & 0 & 0 & x-z & 0 & 0 \\ 0 & -z & 0 & 0 & z^2 & 0 & 0 & -1 & 0 & 0 & x-z & 0 \\ 0 & 0 & -z & 0 & 0 & z^2 & 0 & 0 & -1 & 0 & 0 & x-z \\ -xz & 0 & 0 & 0 & 0 & 0 & -x-z & 0 & 0 & x^2 & 0 & 0 \\ 0 & -xz & 0 & 0 & 0 & 0 & 0 & -x-z & 0 & 0 & x^2 & 0 \\ 0 & 0 & -xz & 0 & 0 & 0 & 0 & 0 & -x-z & 0 & 0 & x^2 \end{pmatrix}.$$

For the use of the lemma, we construct $S_{s_1} = \bigoplus_{i=1}^{s_1} \Delta$ and $H = \left(T S_{s_1}\right)$. Here, $r = 10$.

The syzygy matrix of H is calculated, and by taking the $r = 10$ first rows we obtain U as

$$U = \begin{pmatrix} x & 0 & 0 & -1 & 0 & 0 & y & 0 & 0 & 0 \\ 0 & x & 0 & 0 & -1 & 0 & -y & yz-z^2 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & -1 & 0 & -y+z & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & -y & -xy & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & y & xy-yz+z^2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & y-z & 0 \\ 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 & yz-z^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x & -y+z & 0 & 0 & 0 \\ z & 0 & 0 & 1 & 0 & 0 & -y & -yz & 0 & -xy \\ 0 & z & 0 & 0 & 1 & 0 & y & yz & 0 & xy-yz+z^2 \\ 0 & 0 & z & 0 & 0 & 1 & 0 & 0 & 0 & y-z \end{pmatrix}.$$

Here the number of columns is $u = 10$. We construct $S_s = \bigoplus_{i=1}^{s} \Delta$ and $I = \big(US_s\big)$.

Constructing the syzygy matrix of this and Gröbner reducing the columns we obtain

$$V = \begin{pmatrix} -y & 0 & yz & 0 \\ y & 0 & -z^2 & 0 \\ 0 & 0 & -y+z & 0 \\ 0 & -y & 0 & yz \\ 0 & y & 0 & -z^2 \\ 0 & 0 & 0 & -y+z \\ 0 & -1 & 0 & -x+z \\ -1 & 0 & -x+z & 0 \end{pmatrix}$$

which is the sought presentation matrix for the module $\mathrm{Hom}(M, N)$. This result differs slightly from the one obtained in [AL94] due to the different term order used. △

4.7. Calculations of Ext

Having the tools to describe Hom between two A-modules, we turn our attention to a related functor that plays a fundamental role in homological algebra, namely Ext. It is an example of a so-called *derived functor*. For two A-modules, Ext^i at an index i can be computed using the methods of Section 4.6.

Definition 4.44. Let M, N be A-modules and the following be a free resolution of M:

$$\cdots \xrightarrow{\Gamma_{i+2}} A^{s_{i+1}} \xrightarrow{\Gamma_{i+1}} A^{s_i} \xrightarrow{\Gamma_i} A^{s_{i-1}} \xrightarrow{\Gamma_{i-1}} \cdots \xrightarrow{\Gamma_2} A^{s_1} \xrightarrow{\Gamma_1} A^{s_0} \longrightarrow M_0 \longrightarrow 0\ .$$

Construct the following sequence of Hom modules at index i:

$$\cdots \longleftarrow \mathrm{Hom}(A^{s_{i+1}}, N) \xleftarrow{\circ\Gamma_{i+1}} \mathrm{Hom}(A^{s_i}, N) \xleftarrow{\circ\Gamma_i} \mathrm{Hom}(A^{s_{i-1}}, N) \xleftarrow{\circ\Gamma_{i-1}} \cdots \xleftarrow{\circ\Gamma_1} \mathrm{Hom}(A^{s_0}, N) \longleftarrow 0\ .$$

We then define $\mathrm{Ext}^i(M, N) = \ker\left({}_\circ\Gamma_{i+1}\right) / \operatorname{im}\left({}_\circ\Gamma_i\right)$.

Remark. From the homological definition, $\mathrm{Ext}^0(M, N) = \mathrm{Hom}(M, N)$. Furthermore, since Ext is the quotient of two A-modules, it is an A-module and in particular retains the abelian group structure.

Computing explicit presentations of the objects in the Hom sequence by the method of Section 4.6 we obtain

$$\cdots \longleftarrow A^{u_{i+1}}/L_{i+1} \xleftarrow{T_{i+1}} A^{u_i}/L_i \xleftarrow{T_i} A^{u_{i-1}}/L_{i-1} \longleftarrow \cdots .$$

and can then calculate $\ker\left({}_{\circ}\Gamma_{i+1}\right)$ by Proposition 4.41.

Example 4.45. Let $A = k[x, y, z]$ and consider the A-modules

$$\begin{aligned} I &= \langle x,\ y,\ z\rangle \\ J &= \langle xyz,\ xy + xz + yz,\ x + y + z\rangle \\ L &= \langle -x^2 + x,\ y^2 + z^2,\ z^3\rangle \end{aligned}$$

and let $M = A^1 \oplus I$ and $N = A^3/(J \oplus I \oplus L)$.

A free resolution for M can be calculated as

$$0 \xrightarrow{0} A^1 \xrightarrow{g_1} A^3 \xrightarrow{g_2} A^4 \longrightarrow M \longrightarrow 0$$

with the maps

$$g_1 = \begin{pmatrix} z \\ -y \\ x \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 0 & 0 & 0 \\ -y & -z & 0 \\ x & 0 & -z \\ 0 & x & y \end{pmatrix}.$$

Applying $\mathrm{Hom}(-, N)$, this gives a sequence

$$0 \longleftarrow \mathrm{Hom}(A^1, N) \xleftarrow{\circ g_1} \mathrm{Hom}(A^3, N) \xleftarrow{\circ g_2} \mathrm{Hom}(A^4, N) \longleftarrow 0.$$

The maps $G_1 : A^3 \to A^9$ and $G_2 : A^{12} \to A^9$ induced by ${}_{\circ}g_1 : \mathrm{Hom}(A^3, N) \to \mathrm{Hom}(A^1, N)$ and ${}_{\circ}g_2 : \mathrm{Hom}(A^4, N) \to \mathrm{Hom}(A^3, N)$, respectively, as homomorphisms between free A-modules are as follows:

$$G_1 = \begin{pmatrix} -z & 0 & 0 & y & 0 & 0 & y+z & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -z & 0 & 0 & y & 0 & 0 & -x \end{pmatrix}$$

$$G_2 = \begin{pmatrix} 0 & 0 & 0 & -y & 0 & 0 & -y-z & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -y & 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & -z & 0 & 0 & 0 & 0 & 0 & -y-z & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -z & 0 & 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 0 & 0 & -z & 0 & 0 & y & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -z & 0 & 0 & y \end{pmatrix}.$$

By matrix multiplication we can verify that all compositions are zero.

Further calculations yield that Ext^1 and Ext^2 have the presentation matrices

$$\begin{pmatrix}
z & y & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & z & y & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & z & y & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & z & y & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & z & y & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & z & y & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & z & y & x & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & z & y & x & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & z & y & x
\end{pmatrix}$$

and

$$\begin{pmatrix}
z & y & x & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & z & y & x & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & z & y & x
\end{pmatrix}.$$

These matrices can be conveniently written as E_9 and E_3 for

$$E_j = \bigoplus_{k=1}^{j} \begin{pmatrix} z & y & x \end{pmatrix}$$

so that

$$\mathrm{Ext}^1(M,N) = A^9/\langle E_9 \rangle = A^9/\left\langle \{\text{all variables in all coordinates}\} \right\rangle$$

and

$$\mathrm{Ext}^2(M,N) = A^3/\langle E_3 \rangle = A^3/\left\langle \{\text{all variables in all coordinates}\} \right\rangle.$$

In essence, we have taken the respective ambient free modules of the Ext groups and “killed” every variable x, y, z. These quotient modules behave as cartesian products of copies of the underlying field k and since the scalar multiplication with a $p \in A$ can be replaced by multiplication with $\mathrm{CT}(p) \in k$, they are in fact isomorphic to the vector spaces k^9 and k^3. $\triangle$

5. Coda

The original theory of Gröbner bases for ideals in polynomial rings over a ground field has become an indispensable set of tools for many ordinary algebraic problems. Many of the leading computer algebra systems, including `mathematica,sagemath,macaulay2` and many others incorporate implementations of Gröbner methods.

As indicated in section 4, the central concepts can be straightforwardly restated in the more general context of modules over the polynomial ring. Further generalizations to different algebraic structures are possible. For instance, analogues of Gröbner bases can be introduced in settings where the ground ring is not necessarily a field (see [AL94]) and in settings of differential rings (see [Man91]). Even for non-commutative scenarios such as in the theory of so-called towers of HNN extensions of free groups, analogues of Gröbner bases has been defined (see [BV06]).

The computational properties of the calculation and usage of Gröbner bases are a subject of their own. Significant refinements of the original Buchberger's algorithm treated in Section 3.3 can be introduced using the syzygy theory defined in Section 4.3 as is done in [AL94]. Current work on computations in module theory (such as computing resolutions) making use of induced Schreyer orders (Theorem 4.26) include [EMSS15].

Extrapolating from the success that the theory of Gröbner bases has celebrated since its inception more than half a century ago, it is not controversial to predict an innumerable variety of applications and generalizations to come in the near future.

References

[AL94] William Adams and Philippe Loustaunau. *An introduction to Gröbner bases.* American Mathematical Society, Providence, RI, 1994.

[AM69] Michael Atiyah and Ian Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BV06] Leonid Bokut and Andrei Vesnin. *Gröbner-Shirshov bases for some braid groups.* Journal of Symbolic Computation, volume 41, p. 357–371, 2006.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases.* Springer-Verlag, New York, 1993.

[CLO05] David Cox, John Little, and Donal O'Shea. *Using algebraic geometry.* Springer, New York, second edition, 2005.

[CLO07] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Springer, New York, third edition, 2007.

[DF04] David Dummit and Richard Foote. *Abstract algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[Eis05] David Eisenbud. *The geometry of syzygies.* Springer-Verlag, New York, 2005.

[EMSS15] Burcin Erocal, Oleksandr Motsak, Frank-Olaf Schreyer, and Andreas Steenpass. *Refined Algorithms to Compute Syzygies.* Preprint, ArXiv e-prints, February 2015.

[Lan02] Serge Lang. *Algebra.* Springer-Verlag, New York, third edition, 2002.

[Man91] Elizabeth Mansfield. *Differential Gröbner bases.* 1991. PhD thesis, University of Sydney.

[Mea92] David Mead. *Newton's identities.* The American Mathematical Monthly, volume 99, p. 749–751, 1992.

[MS03] Teo Mora and Massimiliano Sala. *On the Gröbner bases of some symmetric systems and their application to coding theory.* Journal of Symbolic Computation, volume 35, p. 177–194, 2003.

[Pin10] Charles Pinter. *A book of abstract algebra.* Dover Publications, Inc., Mineola, NY, 2010.

[Wei94] Charles Weibel. *An introduction to homological algebra.* Cambridge University Press, Cambridge, 1994.