Conditions for Univariate SAGBI Bases

Rode Grönkvist

June 15 2020

Abstract

This thesis describes the fundaments of SAGBI theory, including definitions, subduction, SAGBI basis verification and construction. A resultant identity is then used to demonstrate some conditions on univariate SAGBI bases for subalgebras generated by two polynomials.

Populärvetenskaplig sammanfattning

En av matematikens stora nyttor är att kunna beskriva saker på ett precist sätt som tillåter beräkningar. Ett centralt redskap för sådana beskrivningar är *baser*, alltså en referensram som saker beskrivs utifrån. Koordinatsystemet på en karta är ett exempel på en bas som gör det lätt att beskriva en punkt exakt med hjälp av några bokstäver och siffror som hänvisar till en referensram. Denna uppsats handlar om baser för mängder av *polynom*, uttryck med en eller flera okända variabler upphöjda till heltal och med koefficienter, exempelvis $x^2 + 2x + 1$. En *SAGBI-bas* är en bas för en familj av polynom med användbara egenskaper, och denna uppsats undersöker när sådana baser existerar och hur de kan konstrueras. Två perspektiv är vägledande: om vi ges en viss familj av polynom, existerar en SAGBI-bas för den familjen, och hur hittar vi den? Om vi å andra sidan utgår ifrån några polynom, utgör de en SAGBI-bas, och i så fall för vilken familj av polynom?
SAGBI-baser är nära besläktade med Gröbner-baser, som är baser för en viss sorts polynomsstruktur. Gröbner- och SAGBI-baser har mängder av tillämpningar, exempelvis för att lösa icke-linjära ekvationssystem, varför det är av intresse att undersöka deras förekomst och egenskaper.

Acknowledgements

I would like to thank my supervisor Victor Ufnarovski for his guidance, and my friends and family for their help, support, TeX wizardry and proofreading.

Contents

Introduction

Gröbner bases were introduced by Bruno Buchberger in 1965 in his Ph.D. thesis [Buc65], and named for his advisor Wolfgang Gröbner. A Gröbner basis is a certain generating set, or basis, for an ideal in a polynomial ring, and Buchberger contributed an algorithm which can produce such a basis for any ideal and which always terminates. This result led to a wide range of applications in computer algebra. The subject of this thesis is the subalgebra analogue to Gröbner bases in ideals, or SAGBI bases for short. A SAGBI basis has similar properties to Gröbner bases, but for subalgebras instead of ideals. The concept was introduced by Robbiano and Sweedler [RS90], and independently by Kapur and Madlener [KM89].

SAGBI bases differ from Gröbner bases in several important ways. Most notably, any ideal, be it finite or infinite, has a finite Gröbner basis which can be determined by Buchberger's algorithm. For subalgebras there is no such guarantee, and there exist subalgebras that lack a finite SAGBI basis. Thus, it is of interest to classify subalgebras that have finite SAGBI basis.

This thesis aims to give an introduction to the theory of SAGBI bases and to investigate SAGBI bases for algebras generated by two univariate polynomials. Several conditions for such bases were described in [Öfv06].

1 Preliminaries

This chapter provides definitions and preliminary results that are necessary foundations for the theory of Gröbner and SAGBI bases. Motivational and explanatory examples will also be given, as well as references for further reading.

1.1 Motivational Examples

Imagine the following game: you are given some polynomials, which make up your building blocks. You are allowed to combine them with each other via common addition and multiplication of polynomials, as well as multiplication by scalars. How do you describe and classify all the polynomials they can, and cannot, be combined into? And how do you figure out if they can combine into some other given polynomial?

Example 1.1. Let f be the polynomial $f = x$. By multiplying and adding f to itself, every polynomial in x can be generated (if $x^0 = 1$ is considered as an empty product). If $f = x^2$, only polynomials with terms of even power can be generated.

Example 1.2. Let $f = x^3 + a_2x^2 + a_1x + a_0$, $g = x^2 + b_1x + b_0$. Can f and g be combined to form a first-degree polynomial? This is the motivating example of [TUÖ03], and the answer is not obvious. We will return to it later, once we have the tools necessary to answer it.

Conversely, imagine that you are given a large set of polynomials. How do you find the smallest set of building blocks which can combine to generate this larger set, given the rules above? Is it even possible to find such a set?

This "smallest generating set" is called a SAGBI basis. SAGBI bases are an analogue to Gröbner bases, which are similar generating sets for polynomial ideals. The questions posed above are of importance in a range of mathematical applications, and run closely parallel to other problems in algebra.

1.2 Monomials and Polynomials

The basic building blocks of Gröbner and SAGBI theory are polynomials and their components, monomials. Throughout the thesis $\Bbbk$ will denote an arbitrary field over which our polynomials are constructed.

The definitions in this chapter are by and large taken from [Tad19], [CLO92], [AL94]

Definition 1.3. Let a be an element of $\Bbbk$, $x_1, x_2, ..., x_n$ be variables and $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{N}$, where $\mathbb{N}$ is the set of non-negative integers (this notation will be used throughout the thesis). A **monomial** is a product of the form

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n}.$$

To compress the notation, let $\mathbf{x} := (x_1, x_2, ..., x_n)$ and $\boldsymbol{\alpha} := (\alpha_1, \alpha_2, ..., \alpha_n)$. Then the above monomial can be expressed as $\mathbf{x}^{\boldsymbol{\alpha}}$. Note that if $\boldsymbol{\alpha} = (0, 0, ..., 0)$, then $\mathbf{x}^{\boldsymbol{\alpha}} = 1$. To avoid using indices when dealing with monomials in few variables, it is conventional to use e.g. x, y, z instead of x_1, x_2, x_3, where $x_1 = x$, $x_2 = y$, $x_3 = z$. This notation will be used in some examples in this thesis.

Definition 1.4. A **polynomial** is a finite linear combination of monomials. Any polynomial f can be expressed as

$$f = \sum_{i=1}^{t} a_i \mathbf{x}^{\boldsymbol{\alpha}_i},$$

or, equivalently,

$$f = a_t \mathbf{x}^{\boldsymbol{\alpha}_t} + ... + a_1 \mathbf{x}^{\boldsymbol{\alpha}_1} + a_0 \mathbf{x}^{\boldsymbol{\alpha}_0}$$

where $\mathbf{x}^{\boldsymbol{\alpha}_i}$ are different monomials and $a_i \in \Bbbk$. If $a_i \neq 0$, $a_i \mathbf{x}^{\boldsymbol{\alpha}_i}$ is called a **term** of f.

1.3 Monomial and Polynomial Structures

The following notation will be used throughout the thesis. The ring of polynomials in the variables $x_1, x_2, ..., x_n$ over $\Bbbk$ is denoted by $\Bbbk[x_1, x_2, ..., x_n]$. The set of all monomials in $\Bbbk[x_1, x_2, ..., x_n]$ is denoted by $\mathcal{M}$ — it will be clear from context which set of polynomials $\mathcal{M}$ is a subset of.

Remark 1.5. The operations on $\Bbbk[x_1, x_2, ..., x_n]$ are common addition and multiplication of polynomials. $\Bbbk[x_1, x_2, ..., x_n]$ equipped with regular addition of polynomials and multiplication with scalars is also a vector space over $\Bbbk$, considering polynomials as vectors. Thus, for $f, g \in \Bbbk[x_1, x_2, ..., x_n]$ and any $\alpha \in \Bbbk$, $f + g \in \Bbbk[x_1, x_2, ..., x_n]$, $\alpha f \in \Bbbk[x_1, x_2, ..., x_n]$. There also exists a zero vector $0 \in \Bbbk[x_1, x_2, ..., x_n]$. Together, this makes $\Bbbk[x_1, x_2, ..., x_n]$ an algebra. Thus, for any $f, g \in \Bbbk[x_1, x_2, ..., x_n]$, $fg \in \Bbbk[x_1, x_2, ..., x_n]$. Notably, this algebra is associative and commutative, and has identity element $1 = \mathbf{x}^0$.

Definition 1.6. A subset $\mathcal{R}$ of an algebra is a **subalgebra** if it is a subring of the ring underlying that algebra and contains $\Bbbk$. Notably, it is also a subspace, contains both 0 and 1, and is closed under the operations of the algebra.

Definition 1.7. Let $\mathcal{G}$ be a nonempty subset of $\Bbbk[x_1, x_2, ..., x_n]$. The set

$$\mathcal{G}_{mon} := \{\prod_{i=1}^{t} g_i^{\alpha_i}, \quad g_i \in \mathcal{G}, \quad \alpha_i \in \mathbb{N}\}$$

is a monoid under multiplication generated by $\mathcal{G}$.

The elements of $\mathcal{G}_{mon}$ are called $\mathcal{G}$-monomials - though the individual g_i may be polynomials in $\Bbbk[x_1, x_2, ..., x_n]$, their products can be understood as monomials in this context. The identity element 1 of this monoid is the empty product $\prod_{i=0}^{0} g_i^{\alpha_i}$, which can also be written g_i^0 for any $g_i \in \mathcal{G}$.

Definition 1.8. Let $\mathcal{G}$ be a nonempty subset of $\Bbbk[x_1, x_2, ..., x_n]$. The subalgebra **generated by** $\mathcal{G}$ is the smallest subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$ that contains $\mathcal{G}$. It is denoted $\Bbbk[\mathcal{G}]$. A subalgebra $\mathcal{R}$ of $\Bbbk[x_1, x_2, ..., x_n]$ is said to be **finitely generated** if there exists a finite subset $\mathcal{G} \subseteq \mathcal{R}$ such that $\mathcal{R} = \Bbbk[\mathcal{G}]$.

Remark 1.9. The elements of a finitely generated subalgebra $\mathcal{R} = \Bbbk[\mathcal{G}]$ can be seen as polynomials as they are exactly the finite $\Bbbk$-linear combinations of the monomials in $\mathcal{G}$.

Definition 1.10. An **ideal** I in $\Bbbk[x_1, x_2, ..., x_n]$ is a subring of $\Bbbk[x_1, x_2, ..., x_n]$ such that for every $g \in I$ and every $f \in \Bbbk[x_1, x_2, ..., x_n]$, $fg \in I$.

Definition 1.11. An ideal $I \subset \Bbbk[x_1, x_2, ..., x_n]$ is a **monomial ideal** if there exists some subset $A \subset \mathcal{M}$ such that I consists of every polynomial f on the form $f = \sum_{i=1}^{t} g_i \mathbf{x}^{\boldsymbol{\alpha}_i}$, where $g_i \in \Bbbk[x_1, x_2, ..., x_n]$ and $\mathbf{x}^{\boldsymbol{\alpha}_i} \in A$. Then, I is said to be **generated** by A, which is denoted as $I = \langle \mathbf{x}^{\boldsymbol{\alpha}_i} : \mathbf{x}^{\boldsymbol{\alpha}_i} \in A \rangle$.

The following important theorem will not be proved here; the interested reader is directed to [CLO92, pp. 70]

Theorem 1.12 (**Dickson's Lemma**). *A monomial ideal* $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}_i} : \boldsymbol{x}^{\boldsymbol{\alpha}_i} \in A \rangle \subset \Bbbk[x_1, x_2, ..., x_n]$ *can be written on the form* $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}_1}, ..., \boldsymbol{x}^{\boldsymbol{\alpha}_t} \rangle$, *where* $\boldsymbol{x}^{\boldsymbol{\alpha}_1}, ..., \boldsymbol{x}^{\boldsymbol{\alpha}_t} \in \mathcal{M}$.

The idea of the proof is to show that the statement holds for polynomial rings in one variable, and then use induction on the number of variables. The significance of Dickson's lemma is that it guarantees the existence of a finite generating set for every monomial ideal in $\Bbbk[x_1, x_2, ..., x_n]$.

1.4 Term Orders

In the one-variable case, the *degree* of monomials and polynomials is used to compare and order them. When presenting a univariate polynomial on the expanded sum form above, the terms are written in order of descending degree. The notion of degree is not immediately transferable to the multivariate case, however: which of the terms x^2y and xy^2 should be written first in a polynomial? To answer this question, the concept of *term order* is needed. First, the definitions of partial and total *orders* are given.

Definition 1.13. Let B be a nonempty set. A **partial order** is a relation $\succeq$ on B that satisfies the following conditions for all $x, y, z \in$B:

(i) $x \succeq x$ (reflexivity),

(ii) $x \succeq y \succeq x \Rightarrow x = y$ (antisymmetry),

(iii) $x \succeq y \succeq z \Rightarrow x \succeq z$ (transitivity).

$\succeq$ is a **total order** if, additionally, for any $x, y \in$B either $x \succeq y$ or $y \succeq x$. If $x \succeq y$ and $x \neq y$, their relation can be expressed as $x \succ y$.

Definition 1.14. A **term order** or **monomial order** is a total order $\succeq$ on $\mathcal{M}$ satisfying the following for any $\mathbf{x^\alpha}$, $\mathbf{x^\beta}$, $\mathbf{x^\gamma} \in \mathcal{M}$:

(i) $\mathbf{x^\alpha} \succeq \mathbf{x^\beta} \Rightarrow \mathbf{x^\alpha x^\gamma} \succeq \mathbf{x^\beta x^\gamma}$,

(ii) $\mathbf{x^\alpha} \succeq 1$, thus 1 is the minimal element of $\mathcal{M}$.

Proposition 1.15. *The common degree ordering*

$$x^\alpha \geq x^\beta \Leftrightarrow \alpha \geq \beta$$

where α and β are nonnegative integers is the only term ordering on a univariate polynomial ring.

Proof. Assume $x^\alpha > x^\beta$, and that $\succeq$ is some other term order such that $x^\beta \succ x^\alpha$. Then

$$x^\alpha > x^\beta \Leftrightarrow x^\beta x^{\alpha-\beta} > x^\beta x^0 \Leftrightarrow x^{\alpha-\beta} > x^0 = 1.$$

Doing the same for $\succeq$ gives

$$x^\beta \succ x^\alpha \Leftrightarrow x^\beta x^0 \succ x^\beta x^{\alpha-\beta} \Leftrightarrow 1 = x^0 \succ x^{\alpha-\beta}.$$

This contradicts the second property of term orders, so $\succeq$ cannot be another term order. □

There are several term orders on multivariate polynomial rings. These term orders require some ordering of the variables, so in the sequel it is assumed that $x_1 > x_2 > ... > x_n$, without loss of generality.

Definition 1.16. Let $\mathbb{k}[x_1, x_2, ..., x_n]$ be a polynomial ring. The **lexicographical order** $>_{lex}$ on $\mathcal{M}$ is defined as follows:
for $\mathbf{x^\alpha}, \mathbf{x^\beta}$ in $\mathcal{M}$:

$$\mathbf{x^\alpha} >_{lex} \mathbf{x^\beta} \Leftrightarrow \text{ the leftmost nonzero entry of } \boldsymbol{\alpha} - \boldsymbol{\beta} \text{ is positive.}$$

The **degree lexicographical order** $>_{deglex}$ is defined as follows:
for $\mathbf{x^\alpha}, \mathbf{x^\beta}$ in M:

$$\mathbf{x^\alpha} >_{deglex} \mathbf{x^\beta} \Leftrightarrow |\boldsymbol{\alpha}| = \sum_{i=1}^{n} \alpha_i > |\boldsymbol{\beta}| = \sum_{i=1}^{n} \beta_i \text{ or}$$
$$|\boldsymbol{\alpha}| = |\boldsymbol{\beta}| \text{ and } \mathbf{x^\alpha} >_{lex} \mathbf{x^\beta}.$$

The **degree-reverse lexicographical order** $>_{degrevlex}$ is defined as follows:
for $\mathbf{x^\alpha}, \mathbf{x^\beta}$ in M:

$$\mathbf{x^\alpha} >_{degrevlex} \mathbf{x^\beta} \Leftrightarrow |\boldsymbol{\alpha}| = \sum_{i=1}^{n} \alpha_i > |\boldsymbol{\beta}| = \sum_{i=1}^{n} \beta_i \text{ or}$$
$$|\boldsymbol{\alpha}| = |\boldsymbol{\beta}| \text{ and the rightmost nonzero entry of } \boldsymbol{\beta} - \boldsymbol{\alpha} \text{ is positive.}$$

Example 1.17. Let $f = x^2yz^3$, $g = xy^3z^4$ and $x > y > z$ ($x = x_1, y = x_2, z = x_3$). Then $f >_{lex} g$ but $g >_{degrevlex} f$. If instead $z > y > x$, $g >_{lex} f$ and $g >_{degrevlex} f$.

The lexicographical order is simple and intuitive to understand - it is the same ordering as is used for words in a dictionary, hence the name. Deglex order also takes into account the total degree, or sum of exponents, of a monomial. Degrevlex order is less intuitive, but makes certain computations with Gröbner and SAGBI bases much more efficient.

Definition 1.18. Let $f = a_1\mathbf{x}^{\boldsymbol{\alpha}_1} + a_2\mathbf{x}^{\boldsymbol{\alpha}_2} + ... + a_n\mathbf{x}^{\boldsymbol{\alpha}_m}$ be a polynomial and let $\succeq$ be a term order with $\mathbf{x}^{\boldsymbol{\alpha}_1} \succ \mathbf{x}^{\boldsymbol{\alpha}_2} \succ ... \succ \mathbf{x}^{\boldsymbol{\alpha}_m}$ and $\alpha_1 \neq 0$.

(i) The **initial**, or **leading monomial** is defined as $in_{\succeq} f = \mathbf{x}^{\alpha_1}$.

(ii) The **leading coefficient** is defined as $lc_{\succeq} f = a_1$.

(iii) The **leading term** is defined as $lt_{\succeq}(f) = lc_{\succeq} f \cdot in_{\succeq} f = a_1\mathbf{x}^{\alpha_1}$.

Remark 1.19. Let $f_i \in \Bbbk[x]$ for $i = 1, 2, ..., m$.

(i) If f_h is the maximum f_i, then $in_{\succeq} f_h \geq in_{\succeq} \sum_{i=1}^{m} f_i$. If f_h is additionally the only maximal f_i, then $in_{\succeq} f_h = in_{\succeq} \sum_{i=1}^{m} f_i$.

(ii) If all f_i are nonzero, then $in_{\succeq} \prod_{i=1}^{m} f_i = \prod_{i=1}^{m} in_{\succeq} f_i$.

In the sequel, multivariate divisibility is used in the sense of [CLO92, pp. 61].

Definition 1.20. Let $f \in \Bbbk[x_1, x_2, ..., x_n], g_1, ..., g_t \in \Bbbk[x_1, x_2, ..., x_n]$. Dividing f by $g_1, ..., g_t$ means expressing it on the form

$$f = a_1 g_1 + ... + a_t g_t + r$$

where $a_1, ..., a_t$ and the remainder r lie in $\Bbbk[x_1, x_2, ..., x_n]$ (note that the a_i are polynomials, not necessarily scalars). If $r = 0$, f is said to be **divisible** by $g_1, ..., g_t$. Otherwise, r is a $\Bbbk$-linear combination of monomials, none of which is divisible by any of $lt_{\succeq} g_1, ..., lt_{\succeq} g_t$.

Note that any $f \in \Bbbk[x_1, x_2, ..., x_n]$ can be expressed on the form above - this will be discussed in more depth in chapter 2, section 2.

Lemma 1.21. *Let $\mathcal{G}$ be a set of monomials $\mathcal{G} \subseteq \mathcal{M}$, and I be a monomial ideal $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha_i}} : \boldsymbol{x}^{\boldsymbol{\alpha_i}} \in \mathcal{G} \rangle$. Then a monomial $\boldsymbol{x}^{\boldsymbol{\alpha}}$ lies in I if and only if $\boldsymbol{x}^{\boldsymbol{\alpha}}$ is divisible by some $\boldsymbol{x}^{\boldsymbol{\alpha_i}} \in \mathcal{G}$.*

Proof. If $\mathbf{x}^{\boldsymbol{\alpha}}$ is a multiple of $\mathbf{x}^{\boldsymbol{\alpha_i}}$ clearly it lies in I. Conversely, if $\mathbf{x}^{\boldsymbol{\alpha}} \in I$, then $\mathbf{x}^{\boldsymbol{\alpha}} = \sum_{i=0}^{t} g_i \mathbf{x}^{\boldsymbol{\alpha_i}}$. Then by the definition of multivariate divisibility, $\mathbf{x}^{\boldsymbol{\alpha}}$ is divisible by at least one $\mathbf{x}^{\boldsymbol{\alpha_i}}$.

Lemma 1.22. *Any strictly decreasing sequence in $\mathcal{M}$ must terminate.*

Proof. Let $\succeq$ be a term order. Assume there is some infinite strictly decreasing sequence $\mathbf{x}^{\boldsymbol{\alpha_1}} \succ \mathbf{x}^{\boldsymbol{\alpha_2}} \succ ...$ in $\mathcal{M}$. Then $I = \langle \mathbf{x}^{\boldsymbol{\alpha_1}}, \mathbf{x}^{\boldsymbol{\alpha_2}}, ... \rangle$ is a monomial ideal. By Dickson's lemma there exist $\mathbf{x}^{\boldsymbol{\alpha_1}}, ..., \mathbf{x}^{\boldsymbol{\alpha_t}}$ such that $I = \langle \mathbf{x}^{\boldsymbol{\alpha_1}}, ..., \mathbf{x}^{\boldsymbol{\alpha_t}} \rangle$, with possible relabelling.

Note that if $\mathbf{x}^{\boldsymbol{\alpha}}, \mathbf{x}^{\boldsymbol{\beta}} \in \mathcal{M}$ and $\mathbf{x}^{\boldsymbol{\alpha}}$ divides $\mathbf{x}^{\boldsymbol{\beta}}$, then $\mathbf{x}^{\boldsymbol{\beta}} \succeq \mathbf{x}^{\boldsymbol{\alpha}}$, since there then must be $\mathbf{x}^{\boldsymbol{\gamma}} \in \mathcal{M}$ such that $\mathbf{x}^{\boldsymbol{\beta}} = \mathbf{x}^{\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\gamma}}$. The definition of term orders guarantees that $\mathbf{x}^{\boldsymbol{\gamma}} \succeq 1$, so $\mathbf{x}^{\boldsymbol{\beta}} = \mathbf{x}^{\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\gamma}} \succeq \mathbf{x}^{\boldsymbol{\alpha}} 1 = \mathbf{x}^{\boldsymbol{\alpha}}$.

Now consider $\mathbf{x}^{\boldsymbol{\alpha_{t+1}}}$, the first term in the sequence smaller than any element of the generating set of I. Since it is clearly in I, it is divisible by some $\mathbf{x}^{\boldsymbol{\alpha_i}} \in \{\mathbf{x}^{\boldsymbol{\alpha_1}}, ..., \mathbf{x}^{\boldsymbol{\alpha_t}}\}$ by lemma 1.21. This means $\mathbf{x}^{\boldsymbol{\alpha_{t+1}}} \succeq \mathbf{x}^{\boldsymbol{\alpha_i}}$ by the argument above. However, this contradicts our assumption that $\mathbf{x}^{\boldsymbol{\alpha_1}} \succ ... \succ \mathbf{x}^{\boldsymbol{\alpha_t}} \succ \mathbf{x}^{\boldsymbol{\alpha_{t+1}}}$, proving the lemma. □

Corollary 1.23. *A term order $\succeq$ is a well-order on $\mathcal{M}$, meaning that every nonempty subset of $\mathcal{M}$ has a least element.*

Proof. Assume there is some subset A of $\mathcal{M}$ that does not have a least element. Pick an element $\mathbf{x}^{\alpha_1} \in A$. Then, since it is not minimal in A, pick $\mathbf{x}^{\alpha_2} \in A$ such that $\mathbf{x}^{\alpha_1} \succ \mathbf{x}^{\alpha_2}$. Since there is no least element of A, this can be repeated infinitely creating a strictly decreasing sequence that does not terminate, contradicting lemma 1.22. □

2 Gröbner and SAGBI Bases

This chapter gives definitions of Gröbner and SAGBI bases and demonstrates some of their properties. The concepts of reduction and S-polynomials, and subduction and T-polynomials respectively, will be shown, and basis generation algorithms will be presented. In many cases, these concepts will be closely analogous between Gröbner and SAGBI bases.

2.1 Definitions and Existence

Definition 2.1. Let $\mathcal{R}$ be a $\Bbbk$-subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$. The **initial algebra** of $\mathcal{R}$ with respect to $\succeq$, denoted by $In_{\succeq}\mathcal{R}$, is a $\Bbbk$-subalgebra generated by $\{in_{\succeq} f : f \in \mathcal{R} - 0\}$. If I is an ideal in $\Bbbk[x_1, x_2, ..., x_n]$, the **ideal of initials** $In_{\succeq} I$ with respect to $\succeq$ is the ideal generated by $\{in_{\succeq} g : g \in I\}$.

Note that initial algebras and ideals of initials are different structures, and that this notation is dependent on whether the underlying set is an algebra or an ideal. This will be stated whenever the notation is used.

Proposition 2.2. *Let $I \subseteq \Bbbk[x_1, x_2, ..., x_n]$ be an ideal and $\mathcal{R}$ be a subset of $\Bbbk[x_1, x_2, ..., x_n]$.*

(i) $Lt_{\succeq} I = \langle lt_{\succeq} g : g \in I \rangle$ is a monomial ideal equal to $In_{\succeq} I$.

(ii) There exist $g_1, ..., g_t \in I$ such that $Lt_{\succeq} I = \langle lt_{\succeq} g_1, ..., lt_{\succeq} g_t \rangle$.

Proof. To show (i), first note that $In_{\succeq} I$ is a monomial ideal. The elements of $Lt_{\succeq} I$ are on the form $lt_{\succeq} g_1 = lc_{\succeq} g_1 \cdot in_{\succeq} g_1$, where $lc_{\succeq} g_1$ is some constant in $\Bbbk$. Let f be any polynomial in $Lt_{\succeq} I$. From the definition of monomial ideals, $f = \sum_{i=1}^{t} h_i \cdot lt_{\succeq} g_i$ where $h_i \in \Bbbk[x_1, x_2, ..., x_n]$. Let $t_i = h_i \cdot lc_{\succeq} g_i$. Then $f = \sum_{i=1}^{t} t_i \cdot in_{\succeq} g_i$, which shows $Lt_{\succeq} I \subset In_{\succeq} I$. The converse inclusion $In_{\succeq} I \subset Lt_{\succeq} I$ follows from $\Bbbk$ being a field and $lc_{\succeq} g_i$ therefore being invertible. Thus $Lt_{\succeq} I = In_{\succeq} I$, so $Lt_{\succeq} I$ is a monomial ideal. For (ii), Dickson's lemma gives that $In_{\succeq} I$ has a finite generating set of monomials $\{in_{\succeq} g_1, ..., in_{\succeq} g_t\}$. It follows from the argument proving (i) that $Lt_{\succeq} I = \langle in_{\succeq} g_1, ..., in_{\succeq} g_t \rangle = \langle lt_{\succeq} g_1, ..., lt_{\succeq} g_t \rangle$.

Remark 2.3. A statement similar to part (ii) of proposition 2.2 holds for initial algebras, with the difference that $In_{\succeq} R$ is not necessarily finitely generated, meaning that the set $g_1, ...$ is not necessarily finite.

These results lead to the following powerful theorem.

Theorem 2.4 (Hilbert's Basis Theorem). *Every ideal $I \subset \Bbbk[x_1, x_2, ..., x_n]$ has a finite generating set $g_1, ..., g_t \in I$.*

Proof. If $I = 0$ it is generated by the set 0 which is finite. Otherwise, by proposition 2.2, there are $g_1, ..., g_t \in I$ such that $Lt_{\succeq} I = \langle lt_{\succeq} g_1, ..., lt_{\succeq} g_t \rangle$. These $g_1, ..., g_t$ will be demonstrated to generate I.
Clearly, $\langle g_1, ..., g_t \rangle \subset I$. To show the opposite inclusion, let $f \in I$ be any polynomial. Multivariate division of f by $g_1, ..., g_t$ gives

$$f = a_1 g_1 + ... + a_t g_t + r$$

where no term in r is divisible by any of $lt_{\succeq} g_1, ..., lt_{\succeq} g_t$. Note that $r = f - (a_1 g_1 + ... + a_t g_t) \in I$, so if $r \neq 0$, then $lt_{\succeq} r \in Lt_{\succeq} I = \langle lt_{\succeq} g_1, ..., lt_{\succeq} g_t \rangle$. But then by lemma 1.21, $lt_{\succeq} r$ is divisible by some $lt_{\succeq} g_i$. This contradicts r being a remainder, so $r = 0$. Thus

$$f = a_1 g_1 + ... + a_t g_t \in \langle g_1, ..., g_t \rangle$$

showing $I = \langle g_1, ..., g_t \rangle$. □

Definition 2.5. Let $\succeq$ be a term order and I be an ideal in $\Bbbk[x_1, x_2, ..., x_n]$. A finite subset $G = [g_1, ..., g_t]$ of I is a **Gröbner basis** for I if

$$Lt_{\succeq} I = \langle lt_{\succeq} g : g \in G \rangle.$$

SAGBI bases, short for "Subalgebra Analogue to Gröbner Bases for Ideals", are generating sets for subalgebras of polynomial rings rather than ideals.

Definition 2.6. Let $\succeq$ be a term order and $\mathcal{R}$ be a subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$. A subset $\mathcal{G}$ of $\mathcal{R}$ is a **SAGBI basis** for $\mathcal{R}$ if

$$In_{\succeq} \mathcal{R} = \Bbbk[in_{\succeq} g : g \in \mathcal{G}].$$

These definitions are very similar, as are indeed many properties of these bases.

The following example illustrates an application of SAGBI bases for a class of polynomials.

Example 2.7. *Symmetric polynomials* are polynomials such that if any of the variables are interchanged, the polynomial does not change. For instance, $xy + yx + 2$ is a symmetric polynomial of two variables. An *elementary symmetric polynomial* f in the variables $x_1, ..., x_n$ is a polynomial such that for some integer $1 < k < n$, f is the sum of every distinct product of k different variables. The elementary symmetric polynomials in the variables x, y, z are $x + y + z$, $xy + yz + zx$, xyz. For any term order $\succeq$, the set $\mathcal{G} \subset \Bbbk[x_1, x_2, ..., x_n]$ such that

$$\mathcal{G} = \{g : g \textit{ is an elementary symmetric polynomial}\}$$

is a SAGBI basis for the set $\mathcal{S}$ of symmetric polynomials in $\Bbbk[x_1, x_2, ..., x_n]$. The initials of the elementary symmetric polynomials will be $x_1, x_1x_2, ..., x_1x_2...x_n$ under any term order where $x_1 \succ x_2 \succ ... \succ x_n$. Let f be any symmetric polynomial in $\Bbbk[x_1, x_2, ..., x_n]$. Since g is symmetric, its initial must be on the form $x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$, where $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_n$. Thus it can be expressed as a $\mathcal{G}$-monomial. This means $In_{\succeq} S = \Bbbk[in_{\succeq} g : g \in \mathcal{G}]$, so $\mathcal{G}$ is a SAGBI basis for $\mathcal{S}$.

2.2 Subduction and Reduction

An important application of both Gröbner and SAGBI bases is the ability to solve membership problems, i.e. answering whether or not a polynomial is an element of some ideal or subalgebra. To do this, the concepts of reduction (for Gröbner bases) or subduction (for SAGBI bases) is needed. Here, only the definition of subduction will be given, but reduction is similar, replacing subalgebras with ideals.[1]

Definition 2.8. Let $\mathcal{R}$ be a subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$, $\mathcal{G} \subseteq \mathcal{R}$ and $\succeq$ be a term order. For $f, f_1 \in \mathcal{R}$, f **subduces** to f_1 via $\mathcal{G}$ **in one step**, written

$$f \xrightarrow{\mathcal{G}} f_1$$

if there is some $g \in \mathcal{G}_{mon}$ (as in definition 1.7) such that $in_{\succeq} f = in_{\succeq} g$ and some $a \in \Bbbk$ such that $lt_{\succeq} f = a \cdot lt_{\succeq} g$. Then $f_1 = f - ag$.

Remark 2.9. The choice of g and a in the above definition causes the leading term of f to be eliminated. Thus, if $f \xrightarrow{\mathcal{G}} f_1$, then either $lt_{\succeq} f_1 = 0$ or $lt_{\succeq} f \succ lt_{\succeq} f_1$.

Definition 2.10. Let $\mathcal{R}$, $\mathcal{G}$, $\succeq$ be as above. For $f, t \in \mathcal{R}$, f **subduces** to t if there exists a chain of one-step subductions from f to t, written

$$f \xrightarrow{\mathcal{G}} f_1 \xrightarrow{\mathcal{G}} ... \xrightarrow{\mathcal{G}} f_{k-1} \xrightarrow{\mathcal{G}} t.$$

In general, the number of subduction steps does not matter, so the above notation will be compressed to $f \xrightarrow{\mathcal{G}} t$ unless otherwise noted.

Remark 2.11. In general, the result of a subduction is not unique. Consider for example $\mathcal{R} = \Bbbk[g_1 = x, g_2 = x + y]$, a subalgebra of a polynomial ring in two variables, with $\succeq$ being the lex term order. Let $f = x^3$. Clearly $f \in \mathcal{R}$, but since $lt_{\succeq} f = lt_{\succeq} g_1^3 = lt_{\succeq} g_2^3 = lt_{\succeq} g_1 g_2^2 = ...$ there are many ways to subduce f over $\mathcal{R}$.

Remark 2.12. Since $lt_{\succeq} f, lt_{\succeq} f_1, ... \in \Bbbk[x_1, x_2, ..., x_n]$ and $lt_{\succeq} f \succ lt_{\succeq} f_1 \succ ...$, any chain of subductions must terminate (cf. lemma 1.22). When a chain of subductions via some set G terminates, some $f_r \in \mathcal{R}$, possibly 0, will remain. This is called the **remainder** or **final subductum** of f via $\mathcal{G}$. Note that $in_{\succeq} f_r \neq in_{\succeq} g$ for every $g \in \mathcal{G}_{mon}$, since it could otherwise be further subduced. Subduction to the final subductum via $\mathcal{G}$ is denoted $f \xrightarrow{\mathcal{G}*} f_r$. The final subductum is not uniquely determined in general, as noted above. Note also that $f - f_r$ is an element of the subalgebra generated by $\mathcal{G}$.

Lemma 2.13. *Let $\mathcal{R}$, $\succeq$ be as above. If $\mathcal{G}$ is a SAGBI basis for $\mathcal{R}$, then $f \xrightarrow{\mathcal{G}*} 0$ if and only if $f \in \mathcal{R}$.*

Proof. Assume $f \in \mathcal{R}$, $f \xrightarrow{\mathcal{G}*} f_r$. Either $f_r = 0$ or $in_{\succeq} f_r \neq in_{\succeq} g$ for every $g \in \mathcal{G}_{mon}$. But since $\mathcal{G}$ is a SAGBI basis for $\mathcal{R}$, $In_{\succeq}\mathcal{R} = \Bbbk[in_{\succeq} g : g \in \mathcal{G}]$, and in particular there is $g \in \mathcal{G}_{mon}$ such that $in_{\succeq} g = in_{\succeq} f$ for every $f \in \mathcal{R}$. Since $f_r \in \mathcal{R}$, f_r must be 0. Assuming that $f \xrightarrow{\mathcal{G}*} 0$, the fact that $f - f_r \in \mathcal{R}$ means $f - 0 = f \in \mathcal{R}$, finishing the proof.

[1] Note that multivariate division as defined in definition 1.20 is equivalent to reduction if one divides by the elements of a Gröbner basis.

Remark 2.14. This lemma gives a solution to the membership problem for subalgebras. To check if a polynomial f is an element of a subalgebra, subduce f over a SAGBI basis for that subalgebra. Then f is a member of that subalgebra if and only if its final subductum is 0. The same method is used for Gröbner bases, again exchanging the subalgebra and SAGBI basis for an ideal and a Gröbner basis.

With this preparation complete and the membership problem addressed, the next goal is to characterise SAGBI bases further. SAGBI bases are clearly useful, but when do they exist, and how does one find or construct them? These questions are the focus of the rest of the thesis.

Definition 2.15. Let $\mathcal{G}$ be a subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$, let $g_i \in \mathcal{G}_{mon}$, $a_i \in \Bbbk \backslash 0$ for $i \in 1, ..., m$, and $f = \sum_{i=1}^{m} a_i g_i$. The **height** of f is equal to $max\{in_{\succeq} g_i\}$ and the **breadth** of f is the number of g_i such $in_{\succeq} g_i$ is equal to the height of f.

Theorem 2.16. *Let $\mathcal{R}$, $\succeq$ be as above and $\mathcal{G}$ be a subset of $\mathcal{R}$. Then the following are equivalent:*

(i) $\mathcal{G}$ is a SAGBI basis for $\mathcal{R}$.

(ii) all $f \in \mathcal{R}$ subduce to 0 over $\mathcal{G}$.

(iii) all $f \in \mathcal{R}$ can be written on the form

$$f = \sum_{i=1}^{t} a_i g_i$$

where $a_i \in \Bbbk$, $g_i \in \mathcal{G}_{mon}$ and f has breadth 1.

Proof. (i) $\Rightarrow$ (ii) is the statement of lemma 2.13. (ii) $\Rightarrow$ (iii) follows from the subduction algorithm. Each step of the subduction $f \xrightarrow{\mathcal{G}} f_r$ uses some $g_{i+1} \in \mathcal{G}_{mon}$, $a_{i+1} \in \Bbbk$ such that $f_{i+1} = f_i - a_{i+1} g_{i+1}$. For any subduction $f \xrightarrow{\mathcal{G}*} f_r$, expand it to $f \xrightarrow{\mathcal{G}} f_1 \xrightarrow{\mathcal{G}} ... \xrightarrow{\mathcal{G}} f_k \xrightarrow{\mathcal{G}} f_r$. Then

$$\begin{aligned} f_1 &= f - a_1 g_1 \\ f_2 &= f_1 - a_2 g_2 = f - a_1 g_1 - a_2 g_2 \\ &... \\ f_r &= f_k - a_{k+1} g_{k+1} = f - a_1 g_1 - ... - a_{k+1} g_{k+1}. \end{aligned}$$

Rearranging the last equation gives $f = \sum_{i=1}^{k+1} a_i g_i + f_r$. However, since f subduces to 0 by assumption, $f_r = 0$. Since $in_{\succeq} f \succ in_{\succeq} f_1 \succ .. \succ in_{\succeq} f_r$ there is only one g_i such that $in_{\succeq} f = in_{\succeq} g_i$, namely g_1, which gives that f has breadth 1. This shows the implication (ii) $\Rightarrow$ (iii). To show (iii) $\Rightarrow$ (i), $In_{\succeq}\mathcal{G}$ must be shown to generate $In_{\succeq}\mathcal{R}$. Let $s \in In_{\succeq}\mathcal{R}, s \neq 0$. Then there is some $f \in \mathcal{R}$ such that $s = in_{\succeq} f$. By assumption, f has a representation $f = \sum_{i=1}^{t} a_i g_i$ where $a_i \in \Bbbk$, $g_i \in \mathcal{G}_{mon}$ for $i = 1, ..., t$. Since f is assumed to have breadth 1, $in_{\succeq} f = max_{i=1,...,t}\{in_{\succeq} g_i\}$. This gives

$$s = in_{\succeq} f = max_{i=1,...,t}\{in_{\succeq} g_i\} = in_{\succeq} \prod_{j=1}^{m} u_j^{\alpha_j}, (u_j \in \mathcal{G}, \alpha_j \in \mathbb{N}) = \prod_{j=1}^{m} in_{\succeq} u_j^{\alpha_j}.$$

This shows that $In_{\succeq}\mathcal{G}$ generates $In_{\succeq}\mathcal{R}$, and proves the implication (iii) $\Rightarrow$ (i). $\square$

Corollary 2.17. *Let $\mathcal{R}$, $\succeq$, $\mathcal{G}$ be as above. If $\mathcal{G}$ is a SAGBI basis for $\mathcal{R}$, then $\mathcal{R} = \Bbbk[\mathcal{G}]$.*

Proof. Since $\mathcal{G} \subseteq \mathcal{R}$ and $\Bbbk[\mathcal{G}]$ is a subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$ it follows that $\Bbbk[\mathcal{G}] \subseteq \mathcal{R}$. To show the opposite inclusion, let $f \in \mathcal{R}$, $f \neq 0$. By theorem 2.16 there is a representation $f = \sum_{i=1}^{t} a_i g_i$ where $g_i \in \mathcal{G}_{mon}$ for $i = 1, ..., t$, meaning $f \in \Bbbk[g_i : g_i \in \mathcal{G}] = \Bbbk[\mathcal{G}]$. Thus $\mathcal{R} \subseteq \Bbbk[\mathcal{G}]$, so $\mathcal{R} = \Bbbk[\mathcal{G}]$.

If some set $\mathcal{G}$ is referred to as a SAGBI basis without reference to some other set, this means it is a SAGBI basis for $\Bbbk[\mathcal{G}]$.

Remark 2.18. Note that a subalgebra need not be finitely generated, and thus need not have a finite SAGBI basis. In fact, even finitely generated subalgebras may not have finite SAGBI basis. Compare this to Gröbner bases, where the Hilbert basis theorem guarantees that every ideal is finitely generated and every ideal can be shown to have finite Gröbner basis. Also, a generating set need not be a SAGBI basis. This situation will be explored further in the next section.

Example 2.19. This example is due to [RS90]. Let $\mathcal{R}$ be a subalgebra of $\Bbbk[x, y]$ (finitely) generated by $f = x + y$, $g = xy$, $h = xy^2$. Then $\mathcal{R}$ does not have finite SAGBI basis with respect to any term order.

To prove this, first note that every polynomial on the form $h_m = xy^m$, $m \geq 1$, is in $\mathcal{R}$, since $h_m = (x + y)xy^{m-1} - (xy)xy^{m-2}$ and $h_1 = xy = g$, $h_2 = xy^2 = h$. On the other hand, for $j \geq 1$ there are no polynomials in $\mathcal{R}$ that contain y^j as a homogeneous component. To see this, note that $\mathcal{R}$ is a graded algebra, which means that if some polynomial in $\mathcal{R}$ has y^j as a homogeneous component then y^j is in $\mathcal{R}$. Since every element of $\mathcal{R}$ is a polynomial in f, g, h, there must then be some such polynomial $r(x + y, xy, xy^2)$ such that $r(x + y, xy, xy^2) = y^j$. Inserting $x = 0$ gives $r(y, 0, 0) = y^j$. This should imply that $r(x, 0, 0) = x^j$ but inserting $y = 0$ gives $r(x, 0, 0) = 0$, a contradiction. Hence, there is no polynomial in $\mathcal{R}$ with y^j as a homogeneous component.

For any monomial order $\succeq$ on $\mathcal{R}$, either $x \succeq y$ or $y \succeq x$. Since $(x + y)xy = x^2y + y^2x$, $\mathcal{R}$ can also be generated by $\{x+y, xy, x^2y\}$, so any reasoning for the case $x \succeq y$ will also hold for $y \succeq x$ with x and y switched. Thus, assume $x \succeq y$ without loss of generality.

From previous argument, $\mathcal{G} = \{x + y, xy, xy^2, ...\} \subseteq \mathcal{R}$. The aim of the example is to show that this set is a SAGBI basis for $\mathcal{R}$ and that there is no finite SAGBI basis for $\mathcal{R}$. First, note that for $j \geq 1$ there are no elements of $\mathcal{R}$ with initial y^j, since $x \succeq y$ means that such an element would have y^j as a homogeneous component which has been shown to be impossible. Thus the initials of elements in $\mathcal{R}$ are on the form x^iy^j with $i \geq 1$. For some such element $p \in \mathcal{R}$, its initial is generated by $\mathcal{G}$:

$$in_{\succeq} p = x^i y^j = in_{\succeq}(x + y)^{i-1} in_{\succeq}(xy^j).$$

Thus, $In_{\succeq}\mathcal{G}$ generates $In_{\succeq}\mathcal{R}$ and so $\mathcal{G}$ is a SAGBI basis for $\mathcal{R}$. If there were some finite SAGBI basis for $\mathcal{R}$, it has some element with initial of maximal y-degree x^iy^k. Now consider some element of $\mathcal{R}$ with initial of y-degree larger than k. This initial clearly cannot be generated by the finite SAGBI basis since there are no elements of it with y^j as a homogeneous component for any $j \geq 1$, and so there cannot be a finite SAGBI basis for $\mathcal{R}$.

Proposition 2.20. *A singleton set $\mathcal{G} = \{g\}$, $g \in \Bbbk[x_1, x_2, ..., x_n]$ is a SAGBI basis for the subalgebra $\Bbbk[\mathcal{G}]$.*

Proof. Any element f in $\Bbbk[\mathcal{G}]$ must be on the form $f = \sum_{i=1}^{t} a_i g^{\alpha_i}$, $a_i \in \Bbbk$, $\alpha_i \in \mathbb{N}$. This means f subduces to 0 over $\mathcal{G}$, since every term in f is a multiple of g. □

Corollary 2.21. *Let $\mathcal{G}$ be a subset of $\Bbbk[x_1, x_2, ..., x_n]$. If there is some element $g_1 \in \mathcal{G}$ such that every $g \in \mathcal{G}$ can be expressed on the form $\sum_{i=1}^{t} a_i g_1^{\alpha_i}$, $a_i \in \Bbbk$, $\alpha_i \in \mathbb{N}$, then $\mathcal{G}$ is a SAGBI basis and $\{g_1\}$ is a SAGBI basis for $\Bbbk[\mathcal{G}]$.*

Proof. Clearly $\Bbbk[g_1] = \Bbbk[\mathcal{G}]$. $\{g_1\}$ is a SAGBI basis due to proposition 2.20. Since $g_1 \in \mathcal{G}$, any subduction over g_1 can also be performed over $\mathcal{G}$, meaning in particular that every polynomial that subduces to 0 over g_1 also subduces to 0 over $\mathcal{G}$. Thus g_1 being a SAGBI basis implies $\mathcal{G}$ is a SAGBI basis. □

Remark 2.22. It follows from corollary 2.21 that a subalgebra may have several, even infinitely many, different SAGBI bases. Trivially, a subalgebra $\mathcal{R}$ is a SAGBI basis for itself. The SAGBI basis with the lowest cardinality is referred to as the **minimal** SAGBI basis.

2.3 Verification and Construction of Bases

Consider a finite subset $\mathcal{G}$ of $\Bbbk[x_1, x_2, ..., x_n]$. It might seem obvious that $\mathcal{G}$ should be a SAGBI basis for $\Bbbk[\mathcal{G}]$, since every element in $\Bbbk[\mathcal{G}]$ is a finite linear combination of the elements of $\mathcal{G}_{mon}$. However, this need not be the case.

Example 2.23. Let $f = x^3$, $g = x^3 + x^2$ generate $\mathcal{G} \subset \Bbbk[x]$. Clearly $x^2 \in \mathcal{G}$, since $g - f = x^3 + x^2 - x^3 = x^2$ is a finite linear combination of g and f. Since $in_{\geq} f = x^3$ and $in_{\geq} g = x^3$ do not generate $in_{\geq} x^2 = x^2$, $\{f, g\}$ is not a SAGBI basis for $\mathcal{G}$.

This example provides an intuition that pairs of $\mathcal{G}$-monomials with the same initial might create complications for SAGBI bases. Indeed, to verify SAGBI bases, the term *critical pairs* is introduced to refer to such pairs.

Definition 2.24. Let $\mathcal{R}$ be a subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$ and $\succeq$ be a term order. A pair of nonzero elements of $\mathcal{R}$ g_1, g_2 such that $g_1 \neq g_2$ is called a **critical pair** if $in_{\succeq} g_1 = in_{\succeq} g_2$, . For this critical pair, there exists $a \in \Bbbk$ such that $in_{\succeq} g_1 = a \cdot in_{\succeq} g_2$. The polynomial $g_1 - a g_2$ is called a **T-polynomial**, also denoted $T(g_1, g_2)$.

Remark 2.25. If g_1, g_2 is a critical pair, then g_2, g_1 is also a critical pair. Since $\Bbbk$ is a field, $T(g_1, g_2) = b \cdot T(g_2, g_1)$ for some $b \in \Bbbk$.

Definition 2.26. A T-polynomial $T(f, g)$ has a **low representation** over $\Bbbk[\mathcal{G}]$ if it can be expressed as a linear combination of $\mathcal{G}$-monomials $\sum_{i=1}^{t} a_i g_i$, $a_i \in \Bbbk$ such that $in_{\succeq} f = in_{\succeq} g \succ in_{\succeq} g_i$ for all i, or equivalently $height(f) = height(g) \succ height(\sum_{i=1}^{t} a_i g_i)$.

Proposition 2.27. *Let $\mathcal{G}$ be a subset of $\Bbbk[x_1, x_2, ..., x_n]$ and $\succeq$ be a term order. $\mathcal{G}$ is a SAGBI basis if and only if every T-polynomial of critical pairs in $\Bbbk[\mathcal{G}]$ subduces to 0 over $\mathcal{G}$. Equivalently, $\mathcal{G}$ is a SAGBI basis if and only if every T-polynomial has a low representation in $\Bbbk[\mathcal{G}]$.*

Proof. Assume first that $\mathcal{G}$ is a SAGBI basis. Since every T-polynomial of elements in $\mathcal{G}$ must be in $\mathcal{G}$, they all subduce to 0 due to theorem 2.16. To show the converse, let f be any element of $\Bbbk[\mathcal{G}]$. Since $in_{\succeq} f \in \mathcal{G}_{mon}$, it can be subduced over $\mathcal{G}$. The result of this subduction is either a T-polynomial of some critical pair in $\mathcal{G}$, in which case it subduces to 0 by assumption, or some other $f' \in \Bbbk[\mathcal{G}]$ for which $in_{\succeq} f' \in \mathcal{G}_{mon}$, $in_{\succeq} f \succ in_{\succeq} f'$. If no subductum of f is the T-polynomial of a critical pair in $\mathcal{G}$, this creates a strictly decreasing sequence in $\mathbb{N}$ which terminates since $\succeq$ is a well-order. Since every subductum $f^{(k)}$ is either a T-polynomial or has initial in $\mathcal{G}_{mon}$, the final subductum must be 0. Thus every $f \in \mathcal{G}$ subduces to 0, and $\mathcal{G}$ is a SAGBI basis by theorem 2.16.

If every T-polynomial subduces to 0, then any T-polynomial $T(f, g)$ can be written on the form $\sum_{i=1}^{t} a_i g_i$, as in theorem 2.16. Here, $in_{\succeq} f = in_{\succeq} g \succ in_{\succeq} T(f, g) \succeq in_{\succeq} g_i$, from similar reasoning as in the proof of theorem 2.15, meaning $T(f, g)$ has a low representation. If every T-polynomial is assumed to have a low representation, then every polynomial in $\Bbbk[\mathcal{G}]$ can be expressed as a sum $\sum_{i=1}^{t} a_i g_i$, and thus every polynomial in $\Bbbk[\mathcal{G}]$ has final subductum 0. This means $\mathcal{G}$ is a SAGBI basis. □

The above proposition gives a method of verifying that some generating set is a SAGBI basis: find all T-polynomials[2] and check if they subduce to 0. This also suggests a method to construct SAGBI bases from generating sets: if there is some T-polynomial in the subalgebra that doesn't subduce to 0, append its final subductum to the SAGBI basis. Then at least that T-polynomial now subduces to 0. This process is repeated until every T-polynomial subduces to 0 (if there is a finite SAGBI basis). The following theorem provides proof that the method works.

Theorem 2.28 (**SAGBI basis construction**). *Let $\mathcal{R}$ be a subalgebra of $\Bbbk[x_1, x_2, ..., x_n]$ and let $\mathcal{G}_0 \subseteq \mathcal{G}_1 \subseteq ... \subseteq \mathcal{G}_i \subseteq ...$ be a sequence of sets such that $\mathcal{G}_0$ generates $\mathcal{R}$, and all T-polynomials of $\Bbbk[\mathcal{G}_i]$ subduce to 0 over $\Bbbk[\mathcal{G}_{i+1}]$. Then $\mathcal{G}_\infty = \cup_{j=0}^{\infty} \mathcal{G}_j$ is a SAGBI basis for $\mathcal{R}$. If $\mathcal{R}$ has finite SAGBI basis, there exists an integer N such that $\mathcal{G}_N$ is a SAGBI basis for $\mathcal{R}$.*

Proof. First note that $\mathcal{G}_{i+1}$ is constructed by appending the final subductums of every T-polynomial in $\Bbbk[\mathcal{G}_i]$ to $\mathcal{G}_i$. Since the final subductum of any T-polynomial in $\Bbbk[\mathcal{G}_i]$ must be in $\mathcal{R}$ for any i, the subset inclusions hold and $\Bbbk[\mathcal{G}_\infty] = \Bbbk[\mathcal{G}_0] = \mathcal{R}$. If $\mathcal{G}_n = \mathcal{G}_{n+1}$ for some n, then every T-polynomial in $\mathcal{G}_N$ subduces to 0 and $\mathcal{G}_n$ is a SAGBI basis by proposition 2.27. Otherwise, for any T-polynomial $T(f, g)$ of $\mathcal{G}_\infty$, one can choose j so large that the final subductum of $T(f, g)$ is an element of $\mathcal{G}_j$, meaning $\mathcal{G}_\infty$ is a SAGBI basis for $\mathcal{R}$. If $\mathcal{R}$ is assumed to have finite SAGBI basis, since $\mathcal{G}_\infty$ is a SAGBI basis for $\mathcal{R}$ there must be some N such that $\mathcal{G}_N$ is the smallest (finite) subset of $\mathcal{G}_\infty$ that is a SAGBI basis. Then every T-polynomial in $\Bbbk[\mathcal{G}_N]$ subduces to 0 and $\mathcal{G}_N = \mathcal{G}_{N+1}$. □

It should again be noted that this process is not guaranteed to generate a finite SAGBI basis. For Gröbner bases in commutative rings, a very similar process is guaranteed to generate a Gröbner basis in a finite number of steps. In noncommutative rings, ideals might not have finite Gröbner bases, this situation is investigated in [Öfv00].

[2]There are ways of reducing the amount of T-polynomials that need to be checked further, discussed in e.g. [Tad19].

2.4 The Univariate Case

For subalgebras of $\Bbbk[x]$, many useful results and simplifications can be achieved by studying the degrees of generators. The results in this section are due to [Tad19].

Lemma 2.29. *Let $\mathcal{R}$ be a subalgebra of $\Bbbk[x]$ and $\succeq$ be a term order. Then*

(i) $A = \{in_{\succeq} f : f \in \mathcal{R}\}$ *is a multiplicative monoid.*

(ii) $B = \{deg(in_{\succeq} f) : f \in \mathcal{R}\}$ *is an additive monoid.*

(iii) a mapping $\alpha : A \to B$ defined by $\alpha(in_{\succeq} f) = deg(in_{\succeq} f)$ is a monoid isomorphism.

Proof. Let f, g be any polynomials in $\mathcal{R}$. Since $in_{\succeq} f \cdot in_{\succeq} g = in_{\succeq} fg$ and $fg \in \mathcal{R}$, (i) holds, and $x^0 = 1$ is the identity element of the monoid. For (ii), $deg(in_{\succeq} f) + deg(in_{\succeq} g) = deg(in_{\succeq} fg)$ and $fg \in \mathcal{R}$, (ii) holds. Here $deg(x^0) = 0$ is the identity element. As for (iii), α is a bijection from A to B and $\alpha(in_{\succeq} f in_{\succeq} g) = deg(in_{\succeq} f in_{\succeq} g) = deg(in_{\succeq} f) + deg(in_{\succeq} g) = \alpha(in_{\succeq} f) + \alpha(in_{\succeq} g)$, so the statement holds.

Theorem 2.30. *Let $\mathcal{R}$, $\succeq$ be as above and $\mathcal{G}$ be a nonempty subset of $\mathcal{R}$. Then the following statements are equivalent:*

(i) $\mathcal{G}$ *is a SAGBI basis for* $\mathcal{R}$.

(ii) $\{in_{\succeq} g : g \in \mathcal{G}\}$ *generates the multiplicative monoid* $\{in_{\succeq} f : f \in \mathcal{R}\}$.

(iii) $\{deg(in_{\succeq} g) : g \in \mathcal{G}\}$ *generates the additive monoid* $\{deg(in_{\succeq} f) : f \in \mathcal{R}\}$

Proof. Let A, B be as in lemma 2.29, and furthermore let C be the multiplicative monoid generated by $\{in_{\succeq} g : g \in \mathcal{G}\}$ and D be the additive monoid generated by $\{deg(in_{\succeq} g) : g \in \mathcal{G}\}$. The aim of the proof is to show that $A = C$ and $B = D$ if and only if $\mathcal{G}$ is a SAGBI basis. The implication (i) $\Rightarrow$ (ii) was shown as part of the proof of theorem 2.16, which also gives the converse implication (ii) $\Rightarrow$ (i). To show (i) $\to$ (iii), let f be any polynomial in $\mathcal{R}$. Since $\mathcal{G}$ is a SAGBI basis, we have

$$\begin{aligned} f \in \mathcal{R} &\Rightarrow in_{\succeq} f \in In_{\succeq} \mathcal{R} \\ &\Rightarrow in_{\succeq} f \in \langle in_{\succeq} g : g \in \mathcal{G} \rangle \\ &\Rightarrow in_{\succeq} f = \sum_{i=1}^{m} a_i \Big(\prod_{j=1}^{t_i} (in_{\succeq} g_{j_i})^{\alpha_{j_i}}\Big), \quad g_{j_i} \in \mathcal{G} \\ &\Rightarrow in_{\succeq} f = \prod_{j=1}^{t_i} (in_{\succeq} g_{j_i})^{\alpha_{j_i}} \text{for some i} \in \{1, ..., m\} \end{aligned}$$

Then $deg(f)$ is clearly equal to $deg(in_{\succeq} g_j)$, which shows $B \subseteq D$. As for the opposite inclusion, $\mathcal{G} \subseteq \mathcal{R} \Rightarrow In_{\succeq} \mathcal{G} \subseteq In_{\succeq} \mathcal{R} \Rightarrow D \subseteq B$.
To show (iii) $\Rightarrow$ (ii), let $f \in \mathcal{R}$. From (iii), $deg(in_{\succeq} f) = \sum_{i=1}^{m} a_i \cdot deg(in_{\succeq} g_i)$, $g_i \in \mathcal{G}$,

$a_i \in \mathbb{N}$. Let α be as in lemma 2.29. Then

$$\begin{aligned} in_{\succeq} f &= \alpha^{-1} deg(in_{\succeq} f) \\ &= \alpha^{-1}(\sum_{i=1}^{m} a_i \cdot deg(in_{\succeq} g_i)) \\ &= \prod_{i=1}^{m} (\alpha^{-1}(deg(in_{\succeq} g_i)))^{a_i} \\ &= \prod_{i=1}^{m} (in_{\succeq} g_i)^{a_i} \end{aligned}$$

Thus, $in_{\succeq} f \in C$, so $A \subseteq C$. For the opposite inclusion, $\mathcal{G} \subseteq \mathcal{R} \Rightarrow C \subseteq A$. □

This theorem gives a simple way to verify SAGBI bases in the univariate case — simply check whether the degrees of the initials of basis elements generate the degrees of the initials of the subalgebra under addition. This gives part of the answer to the question posed in example 1.2: does the subalgebra generated by $f = x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0$, $g = x^2 + b_1 x + b_0$ contain x? If $\{f, g\}$ is a SAGBI basis the answer is no, as $deg(f) = 3$, $deg(g) = 2$ do not generate $deg(x) = 1$ under addition. It would be possible to verify that $\{f, g\}$ is in fact a SAGBI basis by checking the subduction of T-polynomials, but there is a more general proof of this fact that will be explored in the next chapter. Before that, theorem 2.30 leads to one more result for univariate SAGBI bases.

Definition 2.31. A nonempty subset of $\mathbb{N}$ is an **additive subsemigroup** if it is closed under regular addition.

Theorem 2.32. *Every subalgebra $\mathcal{R}$ of $\Bbbk[x]$ has a finite SAGBI basis.*

Proof: Let $B = \{deg(in_{\succeq} f) : f \in \mathcal{R}\}$. B is an additive subsemigroup due to lemma 2.29. From [SS75] every additive subsemigroup is finitely generated. Let $\mathcal{G} = \{g_1, ..., g_m\}$ such that $\{deg(g_1), ..., deg(g_m))\}$ generates B. By theorem 2.30 $\mathcal{G}$ is a finite SAGBI basis for $\mathcal{R}$. □

Remark 2.33. The approach of working with the structure of degrees of SAGBI bases leads to further conditions on univariate SAGBI bases by utilising results from the study of numerical semigroups, as in [Tad19] which gives conditions for when three generators with consecutive degree form a SAGBI basis.

3 Resultants and Univariate SAGBI Bases

This chapter focuses on an application of resultants to the theory of univariate SAGBI bases first described in [TUÖ03], and developed in [Öfv06]. This chapter will largely follow the structure of the latter. Recall example 1.2, restated here, which that article's motivational example:

Example 3.1. Let $f = x^3 + a_2x^2 + a_1x + a_0$, $g = x^2 + b_1x + b_0$. Does the subalgebra generated by f and g contain any first-degree polynomial?

From the results of the previous chapter, it follows that if $\{f, g\}$ is a SAGBI basis, then $\Bbbk[f, g]$ does not contain any first-degree polynomial as the degrees of f and g cannot be added to make 1. To investigate whether $\{f, g\}$ is in fact a SAGBI basis, the T-polynomials of $\Bbbk[f, g]$ must be inspected - if they subduce to 0, then $\{f, g\}$ is a SAGBI basis.

Example 3.2. Let f and g be as above. First, substitute $t = x + \alpha$, which gives

$$\begin{aligned} f =&(t-\alpha)^3 + a_2(t-\alpha)^2 + a_1(t-\alpha) + a_0 = \\ &= t^3 + (-3\alpha + a_2)t^2 + (3\alpha^2 - 2a_2\alpha + a_1)t + C \\ g =&(t-\alpha)^2 + b_1(t-\alpha) + b_0 = t^2 + (-2\alpha + b_1)t + D \end{aligned}$$

where C and D are some constants. Let $2\alpha = b_1$, which eliminates the first-degree term from g. Relabel the constants before the first- and second-degree terms of f as a and b, respectively. The polynomials now have the form

$$\begin{aligned} f =&t^3 + at^2 + bt + C \\ g =&t^2 + D \end{aligned}$$

.

Now, since the question is whether $\{f, g\}$ is a SAGBI basis, the constants C and D can be discarded, as $\Bbbk[f, g] = \Bbbk[(f - C), (g - D)]$ and $in_{\geq}f = in_{\geq}(f - C)$, $in_{\geq}g = in_{\geq}(g - D)$. Furthermore, the problem can be simplified by working with $f - ag$ instead of f, since $\Bbbk[f, g] = \Bbbk[f - ag, g]$ and $in_{\geq}f = in_{\geq}(f - ag)$. This eliminates the second-degree term of f. Let $f' = f - ag + aD - C = t^3 + at$, $g' = g - D = t^2$ and consider the T-polynomial $f'^2 - g'^3$. If this T-polynomial subduces to 0, then every T-polynomial of $\{f, g\}$ will subduce to 0 (as is proven in

lemma 3.15 below). Carrying out the subduction gives

$$\begin{aligned} f'^2 - g'^3 &= t^6 + 2at^4 + a^2t^2 - t^6 & &= 2at^4 + a^2t^2 = h_4 \\ h_4 - 2ag'^2 &= 2at^4 + a^2t^2 - 2at^4 & &= a^2t^2 = h_2 \\ h_2 - a^2g' &= a^2t^2 - a^2t^2 & &= 0 \end{aligned}$$

This shows that $\{f, g\}$ is in fact a SAGBI basis, since every critical pair subduces to 0 no matter what the coefficients in f and g are. Thus, there are no first-degree polynomials in $\Bbbk[f, g]$.

Though the above method gives an answer to the motivating question, it is not very satisfactory. This chapter will show, using the resultant, that two univariate polynomials of relatively prime degree always constitute a SAGBI basis. Some further conditions on SAGBI bases for algebras generated by two generators will also be shown.

3.1 SAGBI Bases and Field Extensions

The connection between resultants and SAGBI bases requires an alternate condition for SAGBI bases, using the theory of field extensions. This section describes the field extensions $\Bbbk \subset \Bbbk(u) \subset \Bbbk(x)$, where $\Bbbk(x)$ is the field of rational functions in the variable x with coefficients in $\Bbbk$ and $\Bbbk(u)$ is the field extension obtained by adjoining some non-constant polynomial u to the field $\Bbbk$. This notation will be used throughout.

Lemma 3.3. *If $d = deg(u) \geq 1$, then $[\Bbbk(x) : \Bbbk(u)] = d$.*

Proof. Let $p(t) = u(t) - u$, $p(t) \in \Bbbk(x)[t]$ where $u(t)$ is the polynomial obtained by replacing x with t in the polynomial u. The strategy of the proof is to show that this p is the minimal polynomial of x over $\Bbbk(u)$ (possibly differing by a constant factor). Since x is a zero of $p(t)$, p is algebraic over $\Bbbk(u)$ and its minimal polynomial has degree less than or equal to d. Since $d \geq 1$, the polynomial ring $\Bbbk[u]$ is isomorphic to the polynomial ring $\Bbbk[x]$, meaning $\Bbbk[u]$ is a unique factorisation domain (UFD) and $\Bbbk(u)$ is its field of fractions. Then, to prove p is irreducible over $\Bbbk(u)$, it suffices to prove it is irreducible over $\Bbbk[x]$ by Gauss' lemma, which states that a polynomial is irreducible in a UFD if and only if it is irreducible in the field of fractions of that UFD and primitive in the UFD.

Assume then, to the contrary, that there is some non-zero polynomial $q \in \Bbbk[u, t]$ such that $\deg(q) = k < d$ and x is a zero of q. Then q can be written on the form

$$q = q_k t^k + q_{k-1} t^{k-1} + ... + q_1 t + q_0$$

where all $q_i \in \Bbbk[u]$. The assumption that x is a zero of q can be written

$$0 = q(x) = q_k x^k + q_{k-1} x^{k-1} + ... + q_1 x + q_o.$$

For this equality to hold, there must be cancellation between terms containing the same power of x. This is not possible: since every q_i belongs to $\Bbbk[u]$ the degrees of

the terms must obey the congruences

$$\begin{aligned} deg(q_k x^k) &\equiv k \bmod d \\ deg(q_{k-1} x^{k-1}) &\equiv k-1 \bmod d \\ &\dots \\ deg(q_o) &\equiv 0 \bmod d \end{aligned}$$

Since $k < d$, these congruence classes are all different, meaning that the highest terms of the different classes cannot cancel. Thus, the assumption that $k < d$ is contradicted, which shows p is the minimal polynomial of x over $\Bbbk(u)$. □

The proof of the following theorem follows the structure laid out in [Ber97].

Theorem 3.4 (**Lüroth's theorem**). *Let $\Bbbk$ be a field, $\Bbbk(x)$ be the field of rational functions in the variable x over $\Bbbk$ and L be some extension of $\Bbbk$ not equal to $\Bbbk$ such that $\Bbbk \subset L \subset \Bbbk(x)$. Then there is some element y in $\Bbbk(x)$ such that $L = \Bbbk(y)$.*

Proof. This proof will follow a similar strategy of considering some rational function in $\Bbbk(x)[t]$ of minimal degree, showing it is the minimal polynomial of x over $\Bbbk(y)$ and L, and finally that $\Bbbk(y) = L$. First note that every element of $\Bbbk(x)[t]$ can be written as $P(x,t)/Q(x)$, where P and Q are relatively prime in $\Bbbk(x)[t]$ and Q is monic in x. This also holds for $u(x) \in \Bbbk(x)$, and any such $u = P(x)/Q(x)$ will henceforth be assumed to have those properties. Let the *height* of $P(x,t)/Q(x)$ denote the maximum of the degree of P in x and the degree of Q in x.

Pick some nonconstant $y \in L, y = P(x)/Q(x)$ such that y has minimal height, $\deg(P) > \deg(Q)$ and P is monic. This is possible since if a $y' = P'(x)/Q'(x)$ in L of minimal height had $\deg(Q') > \deg(P')$, its inverse would have the same height and also be in L, and since $\Bbbk$ is a field P' can easily be made monic. If a $y' = P'(x)/Q'(x)$ of minimal height had $\deg(Q') = \deg(P') = n$, it could be expressed on the form $y' = \frac{ax^n + P''(x)}{x^n + Q''(x)}$ where $P''(x)$ and $Q''(x)$ are some polynomials of degree lower than n. Some manipulation of this expression gives

$$y' = \frac{ax^n + P''(x)}{x^n + Q''(x)} = \frac{ax^n + a(Q''(x) - Q''(x)) + P''(x)}{x^n + Q''(x)} = a + \frac{P''(x) - aQ''(x)}{x^n + Q''(x)}$$

which means the inverse of $y' - a$ is a rational function in L with the desired properties.

Let $f(t) = P(t) - yQ(t)$. This (monic) polynomial $f(t)$ is irreducible in $L[t]$, since if it had some nontrivial factorisation, one of two cases must hold: either one factor is in $\Bbbk[t]$, in which case it would divide both P and Q, contradicting them being relatively prime, or both factors contain x, meaning they have lower height than y. Either case gives a contradiction, meaning f is irreducible in $L[t]$. By Gauss' lemma, it is then also irreducuble in $L(t)$ Since x is clearly a zero of f, this means f is the minimal polynomial of x over L. Note that $\Bbbk(x)$ has dimension $n = height(y) = deg(P)$ over L.

Now consider the simple field extension $\Bbbk(y)$. f will be shown to be irreducible over $\Bbbk[y]$, which means it is also irreducible over $\Bbbk(y)$ due to Gauss' lemma. If f is not irreducible over $\Bbbk[y]$, there is some factorisation $f = f_1 f_2$ such that $f_1, f_2 \in \Bbbk[y]$. Since f has y-degree 1, either f_1 or f_2 must have y-degree 0, meaning it must lie in $\Bbbk$, making f irreducible. Thus f is irreducible in both $\Bbbk[y]$ and $\Bbbk(y)$. Since it has x

as a zero in $\Bbbk(y)$ it must be the minimal polynomial of x over $\Bbbk(y)$ as well, meaning $\Bbbk(x)$ has dimension $n = height(y)$ over $\Bbbk(y)$. Finally, since $\Bbbk(y) \subseteq L$ and $\Bbbk(x)$ has the same dimension over $\Bbbk(y)$ and L, $\Bbbk(y)$ must be equal to L. □

The following lemmata are due to [Tor02].

Lemma 3.5. *For any polynomial $h \in \Bbbk[x]$, $\Bbbk[h] = \Bbbk(h) \cap \Bbbk[x]$*

Proof. It is clear that $\Bbbk[h] \subseteq \Bbbk(h) \cap \Bbbk[x]$. For the opposite inclusion, let $f \in \Bbbk(h) \cap \Bbbk[x]$, meaning there are polynomials a, b such that $f = \frac{a \circ h}{b \circ h}$. Here $\deg(f) = \deg(a)\deg(h) - \deg(b)\deg(h)$ meaning $\deg(h) | \deg(f)$. The inclusion of f in $\Bbbk[h]$ will be shown by induction on the degree of f. Assume $\deg(f) < \deg(h)$. Then $\deg(f) = 0$, so $f \in \Bbbk[h]$. If f has higher degree then there is γ such that $\deg(f) = \gamma\deg(h)$ and $c \in \Bbbk$ such that $f' = f - ch^\gamma$ has lower degree than f. By the induction hypothesis $f' = \frac{a \circ h}{b \circ h} - ch^\gamma$ is in $\Bbbk[h]$ and so f is also in $\Bbbk[h]$, which means $\Bbbk(h) \cap \Bbbk[x] \subseteq \Bbbk[h]$ and completes the proof.

Lemma 3.6. *If $\{F, G\} \subseteq \Bbbk[x]$ is a SAGBI basis and h any polynomial in $\Bbbk[x]$, then $\{f = F \circ h, g = G \circ h\}$ is also a SAGBI basis.*

Proof. Let $\deg(F) = n$, $\deg(G) = m$, $d = gcd(n, m)$ and $n' = n/d$, $m' = m/d$. Since $\{F, G\}$ is a SAGBI basis the T-polynomial $F^{m'} - G^{n'}$ has a low representation $\sum_{i=1}^{t} a_i g_i$, where g_i are $\{F, G\}$-monomials of degree lower than $dm'n'$. Now substitute x for $h(x)$, giving $f^{m'} - g^{n'} = \sum_{i=1}^{t} a_i g_i'$ where g_i' are the $\{f, g\}$-monomials obtained from the substitution of corresponding $\{F, G\}$-monomials. Then $\deg(f^{m'}) = \deg(g^{n'}) = dn'm'\deg(h)$, and any g_i' has degree $\deg(g_i)\deg(h)$. This means $\sum_{i=1}^{t} a_i g_i'$ is a low representation of $f^{m'} - g^{n'}$, so $\{f, g\}$ is a SAGBI basis.

This preparation will lead to a set of equivalences to $\{f, g\}$ being a SAGBI basis. First, however, the resultant is needed.

3.2 The Resultant

Definition 3.7. Let f, g be polynomials of degree n and m respectively in $\Bbbk[x]$, $f = a_n x^n + ... + a_1 x + a_0$, $g = b_m x^m + ... + b_1 x + b_0$ (f and g will be assumed to be of degree n and m respectively throughout this section). The **Sylvester matrix** of f and g is the $(n + m) \times (n + m)$ matrix

$$\begin{pmatrix}
a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0 & 0 & 0 & ... & 0 \\
0 & a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0 & 0 & ... & 0 \\
0 & 0 & a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0 & ... & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & ... & 0 & a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0 \\
b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0 & 0 & 0 & ... & 0 \\
0 & b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0 & 0 & ... & 0 \\
0 & 0 & b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0 & ... & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & ... & 0 & b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0
\end{pmatrix}$$

and the **resultant** $Res(f, g)$ is the determinant of this matrix.

Lemma 3.8. *Two polynomials f and g in $\Bbbk[x]$ have a nontrivial common factor in $\Bbbk[x]$ if and only if $Res(f,g)=0$.*

A proof of this lemma is given in [CLO92, pp.153].

For two polynomials f,g, define the polynomials $F(t)=f(t)-f(x)$, $G(t)=g(t)-g(x)$ in $\Bbbk(x)[t]$. They share the zero x in the field $\Bbbk(x)$ meaning $Res(F,G)=0$ by lemma 3.8.

Definition 3.9. Treating $f(x),g(x)$ as formal variables f,g, define

$$D(f,g)=det\begin{pmatrix} a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0-f & 0 & 0 & ... & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0-f & 0 & ... & 0 \\ 0 & 0 & a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0-f & ... & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & ... & 0 & a_n & a_{n-1} & a_{n-2} & ... & a_1 & a_0-f \\ b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0-g & 0 & 0 & ... & 0 \\ 0 & b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0-g & 0 & ... & 0 \\ 0 & 0 & b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0-g & ... & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & ... & 0 & b_m & b_{m-1} & b_{m-2} & ... & b_1 & b_0-g \end{pmatrix}$$

Lemma 3.10. *$D(f,g)$ has the form*

$$\sum_{(i,j)\in\Delta}\alpha_{i,j}f^ig^j$$

where $\Delta=\{(i,j)\in\mathbb{N}\times\mathbb{N} : in+jm\leq mn\}$ and $\alpha_{i,j}\in\Bbbk$ for all $(i,j)\in\Delta$. Furthermore $\alpha_{m,0}=(-1)^{m(n+1)}b_m^n$ and $\alpha_{0,n}=(-1)^n a_n^m$

Proof. The determinant of a $k\times k$ matrix $C=(c_{i,j})$ can be calculated with the formula

$$det(C)=\sum_{\sigma\in Perm(k)}sign(\sigma)\prod_{l=1}^{k}c_{l,\sigma(l)}$$

where $Perm(k)$ is the set of all permutations on $\{1,...,k\}$. Using this formula for $D(f,g)$ and gathering terms with the same f,g-monomials gives a sum on the form in the statement of the lemma, with $\alpha_{i,j}\in\Bbbk$. Since there are only m f-terms and n g-terms in $D(f,g)$, Δ must be a subset of $\{1,...,m\}\times\{1,...,n\}$. To prove that Δ has the form claimed in the lemma, let S be the subset of $\{1,...,m+n\}\times\{1,...,m+n\}$ consisting of all pairs $(l,\sigma(l))$ in one non-zero term of the determinant formula above, and let i and j denote the number of a_0-f and b_0-g respectively in this product. Since the determinant is a sum of terms on this form, showing that $in+jm\leq mn$ gives the desired conclusion about Δ. Let (l,r) be some element of S, then

$$\sum_{(l,r)\in S}l=\sum_{(l,r)\in S}r=1+...+(m+n)\Rightarrow\sum_{(l,r)\in S}l-r=0$$

which means the terms can be grouped as

$$\sum_{\substack{(l,r)\in S\\ l\leq m}}(r-l)=\sum_{\substack{(l,r)\in S\\ l>m}}(l-r)=s.$$

Now, considering the form of the matrix in $D(f,g)$, for any nonzero term of the formula for $det(C)$ one of two inequalities must hold: if $l \leq m$ then $0 \leq r - l \leq n$, and if $l > m$ then $0 \leq l - r \leq m$. Every element $c_{l,r}$ of the matrix in $D(f,g)$ which does not obey these inequalities is zero, meaning a term of the determinant formula containing such a factor would be zero. This gives the following inequality:

$$in \leq \sum_{\substack{(l,r)\in S \\ l\leq m}} (r-l) = s$$

since each term of the sum is greater than 0, and exactly i terms are equal to n. On the other hand the following inequality also holds:

$$s = \sum_{\substack{(l,r)\in S \\ l> m}} (l-r) \leq m(n-j)$$

since exactly $n-j$ terms of this sum are non-zero, and these terms are all less than or equal to m. Combining these inequalities gives

$$in \leq s \leq m(n-j) \Rightarrow in + jm \leq mn$$

which shows Δ has the form claimed in the statement of the lemma.

To show that $\alpha_{m,0} = (-1)^{m(n+1)} b_m^n$, consider some term of $det(C)$ with f-degree m (in particular, it will contain $(-f)^m$). For this term, $\sigma(i) = n + i$ for $1 \leq i \leq m$. This gives

$$\sum_{\substack{(l,r)\in S \\ l\leq m}} (r-l) = mn = \sum_{\substack{(l,r)\in S \\ l> m}} (l-r)$$

which means that $\sigma(l) = l - m$ for $m + 1 \leq l \leq m + n$. Thus, the corresponding term in the formula for $det(C)$ will be

$$sign(\sigma) b_m^n (-f)^m = sign(\sigma)(-1)^m b_m^n f^m$$

where $sign(\sigma)$ can be calculated as $(-1)^{mn}$ using the conditions on σ described above, which means $\alpha_{m,0}$ is on the form stated in the lemma. The fact that $\alpha_{0,n} = (-1)^n a_n^m$ can be proved in a similar manner. □

Theorem 3.11. *Let f and g be polynomials in $\Bbbk[x]$ of degrees n and m respectively. f and g form a SAGBI basis if the degrees of f and g are relatively prime.*

Proof. Assume for simplicity that f, g are monic. The strategy of the proof is to show that the T-polynomial $f^m - g^n$ has a low representation. Since only two generators are considered, every T-polynomial must be on the form $f^{m^\alpha} - g^{n^\alpha}$, which has low representation if and only if $f^m - g^n$ has low representation, so it suffices to investigate this smallest T-polynomial. Consider then $D(f,g)$ in the form of lemma 3.10. Since m and n are relatively prime, the expression $in + jm \leq mn$ has equality only when $i = m, j = 0$ or $j = n, i = 0$, so the only $\{f,g\}$-monomials of maximal degree mn in the sum are f^m and g^n. This together with the identities on $\alpha_{m,0}$ and $\alpha_{0,n}$ from the lemma means that

$$D(f,g) = \pm(f^m - g^n) + \sum_{(i,j)} \alpha_{(i,j)} f^i g^j$$

where $in + jm < mn$. Since $D(f, g) = 0$, this means that

$$f^m - g^n = \mp \sum_{(i,j)} \alpha_{(i,j)} f^i g^j$$

where the right hand side is a low representation of $f^m - g^n$. □

Finally, the previous sections culminate in the following equivalences:

Theorem 3.12. *Let f and g be polynomials, of degree n and m respectively, in $\Bbbk[x]$. Let $d = gdc(n, m)$. Then the following are equivalent:*

(i) $\{f, g\}$ *is a SAGBI basis,*

(ii) There exists a polynomial h of degree d and polynomials F and G such that $f = F \circ h$, $g = G \circ h$,

(iii) $[\Bbbk(x) : \Bbbk(f, g)] = d$.

Proof. To show (ii) ⇒ (i), note that the degrees of F and G are relatively prime, meaning they are a SAGBI basis by theorem 3.11. Then by lemma 3.6 $\{f, g\}$ is also a SAGBI basis. To show (i) ⇒ (ii), Lüroth's theorem is applied to show that $\Bbbk(f, g)$ must be equal to $\Bbbk(h)$ for some $h \in \Bbbk(x)$. Then $f, g \in \Bbbk(h) \cap \Bbbk[x]$, so by lemma 3.5 $f, g \in \Bbbk[h]$. This means there are F, G such that $f = F \circ h$, $g = G \circ h$. Now h must be shown to be of degree d. Clearly $\deg(h)|\deg(f)$ and $\deg(h)|\deg(g)$ meaning $\deg(h)|d$. On the other hand, h must be in $\Bbbk[f, g]$, and since $\{f, g\}$ is a SAGBI basis, the initial of h is generated by the initials of f, g. This means $\deg(h)$ is a linear combination of $\deg(f)$, $\deg(g)$, so $d|\deg(h)$. Thus $\deg(h) = d$, which completes the implication.

To show (ii) ⇒ (iii), note that by assumption $\Bbbk(f, g) \subseteq \Bbbk(h)$, meaning $[\Bbbk(x) : \Bbbk(f, g)] \geq [\Bbbk(x) : \Bbbk(h)] = d$, where the last equality follow from lemma 3.3. Combining lemma 3.3 and the tower law gives

$$\begin{aligned} n =& [\Bbbk(x) : \Bbbk(f)] = [\Bbbk(x) : \Bbbk(f, g)][\Bbbk(f, g) : \Bbbk(f)] \\ m =& [\Bbbk(x) : \Bbbk(g)] = [\Bbbk(x) : \Bbbk(f, g)][\Bbbk(f, g) : \Bbbk(g)]. \end{aligned}$$

This means $[\Bbbk(x) : \Bbbk(f, g)]|d$, so $[\Bbbk(x) : \Bbbk(f, g)] = d$. Finally, (iii) ⇒ (ii) is given by Lüroth's theorem in combination with the assumption $[\Bbbk(x) : \Bbbk(f, g)] = d$. There must be some $h \in \Bbbk(x)$ such that $\Bbbk(f, g) = \Bbbk(h)$, and by lemma 3.5 f, g are then elements of $\Bbbk[h]$. This means f, g are polynomials in h, and from lemma 3.3 it follows that $\deg(h) = d$. □

Remark 3.13. Theorem 3.12 cannot be extended to more than two generators, as the implication (ii) ⇒ (i) does not hold even for three polynomials. This is noted in [Tor02] who also notes that (i) ⇒ (ii) holds for any finite number of polynomials. As the proof of (ii) ⇔ (iii) can be extended to hold for any amount of polynomials, a similar set of implications for any finite number of polynomials would be (i) ⇒ (ii) ⇔ (iii), as is noted in [Öfv06].

3.3 Algebras Generated by Two Polynomials

It has been previously shown that two polynomials of relatively prime degree form a SAGBI basis. This sections deals with algebras generated by two polynomials that are not of relatively prime degree, and certain SAGBI bases for such algebras. Throughout, f and g will be assumed to be two polynomials in $\Bbbk[x]$ of degree n and m respectively, such that $gcd(n, m) = d, d > 1$. Furthermore, $n' = \frac{n}{d}$ and $m' = \frac{m}{d}$.

To check whether $\{f, g\}$ is a SAGBI basis, one would check if the T-polynomial $f^{m'} - g^{n'}$ subduces to 0. If it does, then $\{f, g\}$ is a SAGBI basis. If it does not, then subduction of $f^{m'} - g^{n'}$ over $\{f, g\}$ gives some nonzero final subductum h such that $l = deg(h) < m'n'd$. The main result of this section is that if d and l are relatively prime, then $\{f, g, h\}$ is a SAGBI basis. First, some preparation is required.

Remark 3.14. To simplify this section, instead of working with T-polynomials directly many proofs will utilise the degrees of the polynomials of the critical pair. For instance, $\{f, g\}$ is a critical pair if and only if $deg(in_{\geq} f^{\alpha}) = deg(in_{\geq} g^{\beta})$ for some α, β which can be expressed equivalently as the Diophantine equation $n\alpha = m\beta$. In a context where the generators are known, only the exponents α, β are needed, and the critical pair $\{f^{\alpha}, g^{\beta}\}$ will be expressed as the coordinates $[(\alpha, 0), (0, \beta)]$.

Lemma 3.15. *Let f, g, m, n, d, n', m' be as defined above. Every T-polynomial in $\Bbbk[f, g]$ is on the form $\pm(f^{km'} - g^{kn'})$ for some $k \in \mathbb{N}$. In terms of coordinates, this corresponds to the critical pairs $[(km', 0), (0, kn')]$ and $[(0, kn'), (km', 0)]$. If $f^{m'} - g^{n'}$ has low representation, every T-polynomial in $\Bbbk[f, g]$ has low representation.*

Proof. Let the coordinates of some critical pair be $[(i_1, i_2), (j_1, j_2)]$. This corresponds to the T-polynomial $f^{i_1}g^{j_1} - f^{i_2}g^{j_2}$, which by cancellation of terms is equal to $\pm(f^i - g^j)$ for some $i, j \in \mathbb{N}$. Consider first the critical pair with coordinates $[(i, 0), (0, j)]$. Then $in = jm \Rightarrow in' = jm' \Rightarrow i = km' \Rightarrow j = kn'$. This means that

$$[(i, 0), (0, j)] = k[(m', 0), (0, n')]$$

with a similar argument for a critical pair on the form $[(0, i), (j, 0)]$, which gives the first statement of the lemma. The second statement follows from considering $in_{\geq}(f^{m'} - g^{n'})$ which is an $\{f, g\}$-monomial of degree lower than $nm' = mn'$. Clearly $in_{\geq}(f^{\alpha m'} - g^{\alpha n'})$ must be the same $\{f, g\}$-monomial to the power α, which has degree lower than $\alpha nm' = \alpha mn'$, meaning $f^{\alpha m'} - g^{\alpha n'}$ has low representation.

Lemma 3.16. *Let m, n, d, m' be as defined above and l be a positive integer such that gcd(l,d) = 1. Then the condition*

$$i_1 n + j_1 m + k_1 l = i_2 n + j_2 m + k_2 l$$

where $0 \leq k_1 \leq k_2 \leq d$, $0 \leq i_1 < m'$ and $0 \leq i_2 < m'$, implies either that $k_1 = k_2$, $i_1 = i_2$ and $j_1 = j_2$, or that $k_2 = d$ and $k_1 = 0$.

Proof. The condition gives that $(k_2 - k_1)l = (j_1 - j_2)m + (i_1 - i_2)n$, meaning that $d|(k_2 - k_1)$. Thus either $k_2 = d$ and $k_1 = 0$, in which case the statement of the lemma follows, or $k_1 = k_2$. In that case, division by d gives $(j_1 - j_2)m' = (i_2 - i_1)n'$. This means $m'|(i_2 - i_1)$, so i_2 must be equal to i_1 by the assumptions made, and so j_1 must also be equal to j_2 □

Lemma 3.17. *Let m, n, d, l, m', n' be as above. If the linear Diophantine equation*

$$i_1 n + j_1 m + k_1 l = i_2 n + j_2 m + k_2 l$$

has a nontrivial solution $[(i_0, j_0, 0), (0, 0, d)]$, where $0 \leq i_0 \leq m'$ and $0 \leq j_0 \leq n'$, then all T-polynomials have low representation if the T-polynomials corresponding to $[(i_0, j_0, 0), (0, 0, d)]$ and $[(0, n', 0), (m', 0, 0)]$ have low representations.

Proof. First, note that if $[a, b]$ and $[b, c]$ are solutions to the equation in the lemma such that $T(a, b)$ and $T(b, c)$ have low representations, then $T(a, c)$ also has low representation. To prove this, recall the notation that $\mathbf{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$. Then

$$T(a, c) = \mathbf{x}^{\boldsymbol{a}} - \mathbf{x}^{\boldsymbol{c}} = \mathbf{x}^{\boldsymbol{a}} + \mathbf{x}^{\boldsymbol{b}} - \mathbf{x}^{\boldsymbol{b}} + \mathbf{x}^{\boldsymbol{c}} = T(a, b) + T(b, c)$$

which proves the statement. Now, let $[(i_1, j_1, k_1), (i_2, j_2, k_2)]$ be some fixed solution of $i_1 n + j_1 m + k_1 l = i_2 n + j_2 m + k_2 l$. If both $k_1 > 0$ and $k_2 > 0$, subtract some multiple of $[(0, 0, 1), (0, 0, 1)]$ from the solution such that at least one of k_1, k_2 is zero. If both k_1 and k_2 are zero, then the T-polynomial is of the form $f^{i_1} g^{j_1} - f^{i_2} g^{j_2}$, which reduces to the case $f^{m'} - g^{n'}$ by lemma 3.15 If one of k_1 and k_2 is nonzero, assume without loss of generality that $k_1 = 0$ and $k_2 > 0$, which gives the equation

$$k_2 l = (i_1 - i_2 n) + (j_1 - j_2) m.$$

Then $d | k_2$, so there is some integer k such that $k_2 = kd$. Let $a = (i_1, j_1, 0)$ and $b = (i_2 + k i_0, j_2 + k j_0, 0)$ and $c = (i_2, j_2, kd)$. Then

$$[a, b] = [(i_1, j_1, 0), (i_2 + k i_0, j_2 + k i_0, 0)]$$

and the corresponding T-polynomial has low representation since it again reduces to the case $f^{m'} - g^{n'}$. The T-polynomial corresponding to the pair

$$[b, c] = [(i_2 + k i_0, j_2 + k j_0, 0), (i_2, j_2, kd)] = [(i_2, j_2, 0), (i_2, j_2, 0)] + k[(i_0, j_0, 0), (0, 0, d)]$$

also has low representation, since the T-polynomial corresponding to $[(i_0, j_0, 0), (0, 0, d)]$ has low representation by assumption, as does the T-polynomial corresponding to $[(i_2, j_2, 0), (i_2, j_2, 0)]$, trivially. Since both $[a, b]$ and $[b, c]$ have low representation, it follows that

$$[(i_1, j_1, 0), (i_2, j_2, kd)] = [a, c]$$

has low representation, as claimed. □

With this preparation done, the main result of the section can be proved.

Theorem 3.18. *Suppose the polynomial h is the final subductum of $f^{m'} - g^{n'}$, i.e.*

$$f^{m'} - g^{n'} = \sum_{(i,j)} \alpha_{(i,j)} f^i g^j + h$$

where $in + jm < m'n'd$ for all terms in the sum. If $deg(h) = l$ and $gcd(l, d) = 1$, then $\{f, g, h\}$ is a SAGBI basis.

Proof. Assume that f and g are monic for simplicity. Consider f, g, h as formal variables, and note that they generate the algebra $\Bbbk[f, g, h]$. The idea of the proof is to use the element

$$t = f^{m'} - g^{n'} - \sum_{(i,j)} \alpha_{(i,j)} f^i g^j - h$$

to subduce $D(f, g)$ in this algebra, which will give a useful identity when passing to $\Bbbk[x]$. These subductions will be performed with respect to deglex order, i.e. $f^{i_1} g^{j_1} h^{k_1} >_{deglex} f^{i_2} g^{j_2} h^{k_2}$ if and only if $i_1 n + j_1 m + k_1 l > i_2 n + j_2 m + k_2 l$ or, in the case of equality, if $f^{i_1} g^{j_1} h^{k_1} >_{lex} f^{i_2} g^{j_2} h^{k_2}$ where $f > g > h$.

Now consider $D(f, g)$ as a polynomial in $\Bbbk[f, g, h]$ and subduce it over $\{t\}$. The result will be some polynomial

$$R(f, g, h) = \sum \gamma_{(i,j,k)} f^i g^j h^k$$

which only contains monomials $f^i g^j h^k$ where $i < m'$, $k \leq d$. The inequality $i < m'$ follows from the fact that $in_{deglex} t = f^{m'}$, so any term of R containing f^s where $s > m'$ can be further subduced. The inequality $k \leq d$ follows from the fact that t has a positive term $f^{m'}$ and a negative term h, meaning that every time a factor h appears during subduction, a factor $f^{m'}$ disappears. Since the only term with maximal f-degree of $D(f, g)$ is $f^m = f^{m'd}$ (from lemma 3.10), the only term with maximal h-degree that will appear during subduction is h^d.

Now replace f, g, h with $f(x), g(x), h(x)$, and note that $R(f, g, h)$ is then 0 (since both $D(f(x), g(x))$ and $t(x)$ are 0 over $\Bbbk[x]$). This gives an identity between $f(x), g(x), h(x)$. In particular, the terms of highest degree in R must cancel, thus at least two $\{f, g, h\}$-monomials must have the same maximal degree. By lemma 3.16, the only $\{f, g, h\}$-monomials that can have the same maximal degree are $f(x)^{i_1} g(x)^{j_1}$ and $f(x)^{i_2} g(x)^{j_2} h(x)^d$ for some $i_1, i_2 < m'$. The fact that the only $\{f, g, h\}$-monomial of h-degree d is $h(x)^d$ implies that $i_2 = j_2 = 0$. Since all other terms of R have lower degree, the equation $R = 0$ can be represented as

$$\alpha f(x)^{i_1} g(x)^{j_1} - \beta h(x)^d = \sum_{(i,j,k) \notin \{(i_1,j_1,0),(0,0,d)\}} \gamma_{(i,j,k)} f^i g^j h^k$$

for some nonzero $\alpha, \beta \in \Bbbk$. The right hand side of this equation is a low representation of the T-polynomial corresponding to $[(i_1, j_1, 0), (0, 0, d)]$ Since the T-polynomial corresponding to $[(m', 0, 0), (0, n', 0)]$ clearly has low representation in terms of f, g, h, lemma 3.17 gives that every T-polynomial over $\{f, g, h\}$ has low representation, meaning $\{f, g, h\}$ is a SAGBI basis. □

There is a partial converse to this theorem.

Theorem 3.19. *Let h be a non-zero $\{f, g\}$-subduced remainder of the T-polynomial $f^{m'} - g^{n'}$ and $\{f, g, h\}$ be a SAGBI basis. If $p = gcd(m, n)$ is a prime, then p and $l = deg(h)$ are relatively prime.*

Proof. To prove the theorem, assume that $\{f, g, h\}$ is a SAGBI basis and, contrary to the statement of the theorem, that $p = gcd(m, n)$ is a prime dividing l. As in the proof of theorem 3.12, combining lemma 3.3 and the tower law gives

$$\begin{aligned} n &= [\Bbbk(x) : \Bbbk(f)] = [\Bbbk(x) : \Bbbk(f, g)][\Bbbk(f, g) : \Bbbk(f)] \\ m &= [\Bbbk(x) : \Bbbk(g)] = [\Bbbk(x) : \Bbbk(f, g)][\Bbbk(f, g) : \Bbbk(g)]. \end{aligned}$$

Thus $[\Bbbk(x) : \Bbbk(f,g)]$ divides $gcd(m,n) = p$, and since p is assumed to be prime either $[\Bbbk(x) : \Bbbk(f,g)] = p$ or $[\Bbbk(x) : \Bbbk(f,g)] = 1$. In the first case, $\{f,g\}$ is a SAGBI basis by theorem 3.12 so $h = 0$, contradicting the assumption. In the second case, $\Bbbk(f,g) = \Bbbk(x)$ which implies that x can be written as a quotient of two polynomials in $\Bbbk[f,g]$. Since $\{f,g,h\}$ is a SAGBI basis, all elements of $\Bbbk[f,g,h] = \Bbbk[f,g]$ have degree divisible by p, in particular the numerator and denominator of x (considered as a quotient). This means x has degree divisible by p which is not possible, and so we have a contradiction, which shows that the theorem holds. □

Remark 3.20. Note that this theorem does not hold if p is not assumed to be prime.

Example 3.21. Let f and g be univariate polynomials such that $\deg(f) = n = 9$, $\deg(g) = m = 6$, and let h be the final subductum of $T(f,g) = f^2 - g^3$. If h is 0, then every T-polynomial of $\{f,g\}$ subduces to 0 and $\{f,g\}$ is a SAGBI basis. If h is nonzero, it has degree lower than $2n = 3m = 18$, and if that degree is relatively prime to 3, then $\{f,g,h\}$ is a SAGBI basis by theorem 3.18. The case where $\deg(h)$ is a multiple of 3 must be considered next. Clearly h cannot have degree 6, 9, 12 or 15, since it could then be further subduced by g, f, g^2 and fg respectively. So, if $\deg(h) = 3$, is $\{f,g,h\}$ ever a SAGBI basis? Consider the T-polynomials $h^3 - f$, $h^2 - g$. If these are both 0, then both f and g are polynomials in h, meaning that $\{f,g\}$ is a SAGBI basis by theorem 3.12. If either of them is nonzero, then not all T-polynomials in $\{f,g,h\}$ subduce to 0, and so $\{f,g,h\}$ is not a SAGBI basis. Thus, if $\deg(h) = 3$, $\{f,g,h\}$ is never a minimal SAGBI basis.

Example 3.22. The last case described in the previous example is illustrated in the simple example of $f = x^9$, $g = x^6 + x$. Then $f^2 - g^3 = x^3$ which cannot be further subduced, so let $x^3 = h$. Then $h^3 - f = 0$ but $h^2 - g = x$, which cannot be further subduced, so let $x = u$. Now every T-polynomial over $\{f,g,h,u\}$ can be subduced to 0 and $\{f,g,h,u\}$ is a SAGBI basis for $\Bbbk[f,g] = \Bbbk[x]$. Note that due to corollary 2.21, $\{u\} = \{x\}$ is a SAGBI basis for $\Bbbk[f,g]$, and is in fact the minimal SAGBI basis.

Future Research

The classification of subalgebras with finite SAGBI bases is an open problem, meaning that further research into conditions for generators to form a finite SAGBI basis would be useful - an approach that uses results from the study of numerical semigroups is suggested in [Tad19], and could be developed further. An alternative approach to the membership problem for subalgebras was suggested by my supervisor, Victor Ufnarovski. The idea, which is illustrated in the example below, is to find function conditions on the evaluation of polynomials to determine whether they are generated by some SAGBI basis.

Example 3.23. Let $f = x^3 - x$ and $g = x^2$ where $f, g \in \Bbbk[x]$. Let h be some other polynomial in $\Bbbk[x]$. To determine whether h lies in $\Bbbk[f, g]$, one could subduce it over $\{f, g\}$. On the other hand, note that any term of even power in h is generated by g, meaning that only terms of odd power have bearing on whether h lies in $\Bbbk[f, g]$. Form the polynomial $h_{odd} = \frac{h(x)-h(-x)}{2}$, which contains only the odd-powered terms of h. If h_{odd} lies in $\Bbbk[f, g]$, it will consist of linear combinations of terms on the form $(x^3 - x)^i(x^2)^j$. This gives the simple condition $h \in \Bbbk[f, g] \Leftrightarrow h_{odd}(1) = 0 \Leftrightarrow h(1) = h(-1)$.

This example could be expanded to e.g. $f = x^3 + ax$, where a is some nonzero scalar, via variable substitution. It is still not clear that the method can be generalised, but the idea of finding conditions on evaluations of polynomials as a way of testing their membership is novel and could potentially be much quicker than performing subductions, were such conditions to be found.

Bibliography

[AL94] William Adams and Philippe Loustaunau. *An introduction to Gröbner bases*. Providence, R.I: American Mathematical Society, 1994. ISBN: 9780821838044.

[Ber97] G. Bergman. *Luroth's Theorem and some related results, developed as a series of exercises*. Lecture notes, University of California, Berkeley. https://math.berkeley.edu/ gbergman/grad.hndts/. 1997.

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

[CLO92] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer International Publishing, 1992. DOI: 10.1007/978-3-319-16721-3.

[KM89] Deepak Kapur and Klaus Madlener. "A Completion Procedure for Computing a Canonical Basis for a k-Subalgebra". In: *Computers and Mathematics*. Springer US, 1989, pp. 1–11. DOI: 10.1007/978-1-4613-9647-5_1.

[Öfv00] Hans Öfverbeck. "Canonical Bases in Noncommutative Algebras". MA thesis. Lund University, 2000.

[Öfv06] Hans Öfverbeck. "Constructive methods for SAGBI and SAGBI-Gröbner bases". PhD thesis. Lund, 2006. ISBN: 9162867709.

[RS90] Lorenzo Robbiano and Moss Sweedler. "Subalgebra bases". In: *Commutative Algebra*. Springer Berlin Heidelberg, 1990, pp. 61–87. DOI: 10.1007/bfb0085537.

[SS75] William Y. Sit and Man-Keung Siu. "On the Subsemigroups of n". In: *Mathematics Magazine* 48.4 (Sept. 1975), pp. 225–227. DOI: 10.1080/0025570x.1975.11976495.

[Tad19] Dawit Solomon Tadesse. "A SAGBI Basis For Some Subalgebras Of Polynomial Rings". PhD thesis. Addis Ababa University, 2019.

[Tor02] Anna Torstensson. "Canonical Bases for Subalgebras on two Generators in the Univariate Polynomial Ring". English. In: *Beitrage zur Algebra und Geometrie* 43.2 (2002), pp. 565–577. ISSN: 0138-4821.

[TUÖ03] Anna Torstensson, Victor Ufnarovski, and Hans Öfverbeck. "On SAGBI basis and Resultants." English. In: *Nato Science series Mathematics,Physics and Chemistry*. Ed. by Jurgen Herzog and Victor Vuletescu. Vol. 115. 2003, pp. 241–254.