Applicable Algebra in Engineering, Communication and Computing (2022) 33:751–789
https://doi.org/10.1007/s00200-022-00573-4

ORIGINAL PAPER

Subalgebras in $K[x]$ of small codimension

Rode Grönkvist[1] · Erik Leffler[1] · Anna Torstensson[1] · Victor Ufnarovski[1]

Received: 21 October 2021 / Revised: 29 June 2022 / Accepted: 15 July 2022 /
Published online: 20 August 2022

Abstract
We introduce the concept of subalgebra spectrum, $Sp(A)$, for a subalgebra A of finite codimension in $\mathbb{K}[x]$. The spectrum is a finite subset of the underlying field. We also introduce a tool, the characteristic polynomial of A, which has the spectrum as its set of zeroes. The characteristic polynomial can be computed from the generators of A, thus allowing us to find the spectrum of an algebra given by generators. We proceed by using the spectrum to get descriptions of subalgebras of finite codimension. More precisely we show that A can be described by a set of conditions that each is either of the type $f(\alpha) = f(\beta)$ for α, β in $Sp(A)$ or of the type stating that some linear combination of derivatives of different orders evaluated in elements of $Sp(A)$ equals zero. We use these types of conditions to, by an inductive process, find explicit descriptions of subalgebras of codimension up to three. These descriptions also include SAGBI bases for each family of subalgebras.

Keywords Subalgebra spectrum · SAGBI basis · Derivation · Resultant

Mathematics Subject Classification 13P05 · 13P10 · 13P15 · 12H05

1 Introductory examples

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero and A be a unital subalgebra in $\mathbb{K}[x]$. To begin with we give several non-trivial examples of such subalgebras.

✉ Anna Torstensson
anna.torstensson@math.lth.se

Rode Grönkvist
rodejg@gmail.com

Erik Leffler
er1110le-s@student.lu.se

Victor Ufnarovski
victor.ufnarovski@math.lth.se

[1] Centre for Mathematical Sciences, Lund Universtiy, Lund, Sweden

Example 1 $A = \{f(x) | f'(0) = f''(0) = f^{(5)}(0) = 0\}$.

Example 2 Let ε be a primitive root of order 8.

$$A = \{f(x) | f(1) = f(-1), f(\varepsilon) = f(\varepsilon^7), f(\varepsilon^3) = f(\varepsilon^5)\}.$$

Example 3 Let ε be a primitive root of order 12.

$$A = \{f(x) | f'(0) = 0, f(\varepsilon) = f(\varepsilon^5), f(\varepsilon^7) = f(\varepsilon^{11})\}.$$

Example 4 Let ε be a primitive root of order 3.

$$A = \{f(x) | f(1) = f(\varepsilon) = f(\varepsilon^2), f'(1) + \varepsilon^2 f'(\varepsilon) + \varepsilon f'(\varepsilon^2) = 0\}.$$

It is not difficult to verify directly that we really get subalgebras. One can check that in fact, if given by generators, they are:

$$1)\ \langle x^4, x^3 \rangle\ 2)\ \langle x^4, x^3 - x \rangle\ 3)\ \langle x^4 - x^2, x^3 \rangle\ 4)\ \langle x^4 - x, x^3 \rangle.$$

We want to find general principles for how descriptions using conditions in our examples relate to descriptions in terms of generators and other characteristics of subalgebras.

We restrict ourselves to unital subalgebras of finite codimension n and give a classification for small n. Note that a unital subalgebra in $\mathbb{K}[x]$ is commutative, associative and contains all constants.

2 SAGBI bases and type

One of our aims is to get a deeper understanding of the structure of SAGBI bases, for example to find ways to add an extra element to a SAGBI basis in ways that result in a new SAGBI basis. For this reason we remind the reader of some definitions, which we adapt to our univariate situation. More general definitions can be found for example in [1, 2] or [3].

If A is a subalgebra in $\mathbb{K}[x]$ the set S of all possible degrees of the non-constant polynomials in A form a **numerical semigroup** (that is an additive semigroup consisting of positive integers). It is well-known that such a semigroup is finitely generated. For any finite generating set we can find a finite set of polynomials G such that our set is exactly $\{\deg g_i | g_i \in G\}$. We call G a **SAGBI basis** for A. A proper subset of G can be a SAGBI basis itself, but if there are no such subsets we say that G is **minimal**.

For any non-constant polynomial f of degree $s \in S$ we can find a product $g = \prod_{g_i \in G} g^{c_i}$ such that $\deg g = \sum c_i \deg g_i = s$. Forming $f - \alpha g$ with a suitable constant $\alpha \in \mathbb{K}$ we can obtain a polynomial of smaller degree. We call this operation **subduction**. If the degree of the obtained polynomial still belongs to S, then we can perform another subduction. The importance of the SAGBI basis lies in the fact that $f \in A$ if and only if there exists a sequence of subductions reducing f to a constant.

Let A be an algebra in $\mathbb{K}[x]$ of finite codimension. We define its **type**$T(A) = (d_1, \ldots, d_s)$ as the ordered list of degrees d_i of the elements of a minimal SAGBI basis. Thus the numbers d_i are simply the generators of the numerical semigroup $S = \{\deg f(x) | f(x) \in A\}$. The type is uniquely determined and for a fixed small codimension we can easily enumerate all possible types. For example, there is only one possible type (2, 3) for codimension one and two types, namely (2, 5) and (3, 4, 5) for codimension two. For codimension three the possible types are:

$$(2, 7), (3, 4), (3, 5, 7), (4, 5, 6, 7).$$

3 Monomial subalgebras

As we have seen Example 1 in fact describes the subalgebra generated by x^4 and x^3. This result can easily be generalised.

Theorem 1 *Let A be a* **monomial subalgebra**, *thus A is spanned over $\mathbb{K}$ by monomials $\{x^s, s \in S\}$, where S is a numerical semigroup. Then $f(x) \in A$ if and only if $f^{(i)}(0) = 0$ for each i that does not belong to S.*

Proof First we check that the derivative conditions describe a subalgebra A'. The conditions are linear so we need only to make sure that if $f(x)$ and $g(x)$ satisfy the conditions then the same is true for the product $f(x)g(x)$. Indeed if $i \notin S$ then we have

$$(fg)^{(i)} = \sum_j \binom{i}{j} f^{(j)} g^{(i-j)}$$

and either j or $i - j$ does not belong to S (otherwise $i \in S$) and in any case we obtain that $f^{(j)}(0)g^{(i-j)}(0) = 0$. Secondly we see directly that any monomial $x^s, s \in S$ satisfies the conditions. In fact only the monomials x^i with $i \notin S$ do not satisfy the conditions. So certainly $A \subseteq A'$, but we can say more: if $f(x) \in A'$ then subduction by A reduces $f(x)$ to another polynomial that satisfies the conditions but is a linear combination of the monomials x^i with $i \notin S$. Such a polynomial must be zero and therefore $f(x) \in A$ and $A' \subseteq A$. We conclude that $A' = A$. □

Here is another useful property of monomial algebras.

Theorem 2 *Let $A = \langle x^{a_1}, x^{a_2}, \ldots, x^{a_t} \rangle$ be a monomial subalgebra. There exists $\alpha \neq \beta$ such that $f(\alpha) = f(\beta)$ for all $f(x) \in A$ if and only if $d = gcd(a_1, a_2, \ldots, a_t) > 1$.*

Proof If $d > 1$ let ε be a primitive d-th root of unity, $\varepsilon^d = 1$. Then we can choose arbitrary nonzero β and $\alpha = \varepsilon\beta$ to get $f(\alpha) = f(\beta)$ for all $f(x) \in A$.

For the opposite direction suppose that $f(\alpha) = f(\beta)$ for all $f(x) \in A$ with $\alpha \neq \beta$. Note that $\beta \neq 0$. Let $d = \sum c_i a_i$ for some coefficients $c_1, \ldots c_n$ guaranteed to exist by the Euclidean algorithm. Then

$$\left(\frac{\alpha}{\beta}\right)^{a_i} = 1 \Rightarrow \left(\frac{\alpha}{\beta}\right)^{d} = \prod \left(\left(\frac{\alpha}{\beta}\right)^{a_i}\right)^{c_i} = 1 \Rightarrow d > 1.$$

□

Note that if $d > 1$ then the subalgebra A is contained in $\mathbb{K}[x^d]$ and therefore it has infinite codimension. Such A are outside the scope of our work.

4 Subalgebras of codimension one

Next, let us look at subalgebras of codimension one (in $\mathbb{K}[x]$). Although relatively simple, these algebras give some insight. Obviously such subalgebras have type (2, 3) thus they contain polynomials of degree 2 and 3, which generate our subalgebra. Using variable substitution we can restrict ourselves to the case where the polynomial of degree two is x^2. (Note that all constants are always in any subalgebra). Now the polynomial of degree three can be chosen as $x^3 - ax$. (Again, the constants are not essential and bx^2 can be subtracted). If $a = 0$ then we get a monomial case and know how to describe it from Theorem 1.

If $a \neq 0$ then the replacement $x \to \alpha x$ with $\alpha^2 = a$ reduces the situation to the case $x^3 - x$. So it is sufficient to study the subalgebra $A = \langle x^3 - x, x^2 \rangle$. Note that for each odd $k > 1$ we have $x^k - x = (x^{k-2} - x)x^2 + (x^3 - x) \in A$ by induction. So $f(x) = \sum a_i x^i$ can be subduced to cx where $c = a_1 + a_3 + a_5 + \cdots$. Thus $f(x) \in A \Leftrightarrow c = 0 \Leftrightarrow f(1) - f(-1) = 0$. This gives us the following result:

Theorem 3 *For any subalgebra A of codimension one either there exists γ such that $f(x) \in A \Leftrightarrow f'(\gamma) = 0$ or there exists $\alpha \neq \beta$ such that $f(x) \in A \Leftrightarrow f(\alpha) = f(\beta)$.*

Proof We only need to recover the old variable. Then the monomial case corresponds to the first case and $f(1) = f(-1)$ to the second. □

The above theorem already displays some ideas that we will try to generalise later on.

5 Derivations

Definition 1 Let $\alpha \in \mathbb{K}$. A linear map $D : A \to \mathbb{K}$ is called an α-**derivation** if it satisfies the condition

$$D(f(x)g(x)) = D(f(x))g(\alpha) + f(\alpha)D(g(x))$$

for any $f(x), g(x) \in A$. We simply call it a **derivation** if it is an α-derivation for some α.

A simple example is **trivial derivation** $f(x) \to cf'(\alpha)$. For $A = \mathbb{K}[x]$ we have only trivial α-derivations (with $c = D(x)$), but as we will see later we can find other derivations in proper subalgebras.

Note that the set of α-derivations is a vector space over $\mathbb{K}$, but the set of all derivations on A is not. Nevertheless it is important for the future to note that a β-derivation is also an α-derivation if $f(\alpha) = f(\beta)$ for any $f(x) \in A$.

Now we can formulate an important result obtained in [4], that will turn out to be pivotal for our continued exploration.

Theorem 4 *Any subalgebra A of codimension $n > 1$ is contained in a subalgebra B of codimension $n - 1$. Moreover A can be defined in B either as the kernel of some α -derivation of B or as $A = \{f(x) \in B | f(\alpha) = f(\beta)\}$ for some $\alpha, \beta \in \mathbb{K}$.*

Note that in [4] derivations are defined in a more general way, by the condition $D(fg) = D(f)\varphi(g) + \varphi(f)D(g)$, for some ring homomorphism $\varphi : B \to \mathbb{K}$. But in the same article it is shown that any homomorphism $A \to \mathbb{K}$ can be lifted to a homomorphism $B \to \mathbb{K}$. Induction over codimension shows that in our situation such an algebra homomorphism is simply a homomorphism $\mathbb{K}[x] \to \mathbb{K}$ which is nothing else than a map $f(x) \to f(\alpha)$ for some $\alpha \in \mathbb{K}$. For that reason we can use α-derivation in our reformulation.

We are thankful our referee for the following important remark. We can introduce more general (α, β)-derivations as maps $D : B \to \mathbb{K}$ such that

$$D(f(x)g(x)) = f(\alpha)Dg(x) + D(f(x))g(\beta)$$

and still have $A = \ker D$ as a subalgebra. Thus we can consider the map $f(x) \to f(\alpha) - f(\beta)$ as (α, β)-derivation and α-derivations as (α, α)-derivation which explains why many of our proofs below are quite similar for both alternatives. In fact his comments give much deeper generalisation, but we restrict ourselves by this remark only.

6 Subalgebra conditions

A straightforward induction argument using Theorem 4 shows that any subalgebra A of codimension n can be described by n linear conditions $L_i(f) = 0$ where L_i is either a derivation of some subalgebra containing A or has the form $L_i(f) = f(\alpha_i) - f(\beta_i)$ for some constants $\alpha_i, \beta_i \in \mathbb{K}$.

Our main hypothesis when initiating this work (which will be proved later) was that linear conditions defining subalgebras can be stated in a neater way. Namely, we hoped that for any subalgebra of finite codimension m there would exist a finite set, which we will call the spectrum of the algebra, and m linear conditions expressed in terms of $f(x)$ and finitely many derivatives $f^{(k)}$ evaluated in the elements of the spectrum which determine if $f(x) \in A$. We have seen such conditions in Theorems 1 and 3 and in Examples 1–4 and want to understand their nature.

We want them to be **subalgebra conditions**. By this we mean that the set of all polynomials satisfying the conditions form a subalgebra. Since our conditions are linear we only need to demand two things for them to be subalgebra conditions. Firstly, a trivial one: that constants should satisfy the conditions. Secondly, a non-trivial one: that whenever $f(x)$ and $g(x)$ satisfy the conditions, so does the product $f(x)g(x)$.

For example the condition $f(\alpha) = 0$ is not a subalgebra condition, because the non-zero constants do not satisfy it. But the condition $f(\alpha) = f(\beta)$ is a subalgebra condition. The same is true for the condition $f'(\alpha) = 0$.

The single condition $f'(\alpha) + f'(\beta) = 0$ is not a subalgebra condition, but together the conditions $f(\alpha) = f(\beta), f'(\alpha) + f'(\beta) = 0$ are subalgebra conditions. As this example shows being subalgebra conditions is a property of a *set* of conditions. (The set may, however, as in the first two examples, consist of just one element.)

In general, any condition $\sum c_i f'(\alpha_i) = 0$ combined with $f(\alpha_1) = f(\alpha_2) = \cdots = f(\alpha_k)$ gives a set of subalgebra conditions.

Indeed since the conditions are linear we only need to check that if $f(x)$ and $g(x)$ satisfy the conditions then the same is true for $f(x)g(x)$. We have

$$\begin{aligned}\sum c_i (fg)'(\alpha_i) &= \sum c_i f'(\alpha_i) g(\alpha_i) + c_i f(\alpha_i) g'(\alpha_i) \\ &= \Big(\sum c_i f'(\alpha_i)\Big) g(\alpha_1) + f(\alpha_1)\Big(\sum c_i\, g'(\alpha_i)\Big) = 0.\end{aligned}$$

One can find generalisations including derivatives of higher order, but we skip this for now and show only one spectacular example of subalgebra conditions:

$$f'(0) = 0; \quad f'''(0) = 3f''(0); \quad f^{(5)}(0) = 10 f^{(4)}(0).$$

7 Spectrum

Now we want to introduce the main definition of this article.

Definition 2 Let A be a subalgebra of finite codimension. Its **spectrum** consists of $\alpha \in \mathbb{K}$ such that either $f'(\alpha) = 0$ for all $f(x) \in A$ or there exists $\beta \neq \alpha$ such that $f(\alpha) = f(\beta)$ for all $f(x) \in A$. In the second case β obviously belongs to the spectrum as well. We write $Sp(A)$ to denote the spectrum of the algebra A.

Unfortunately the word spectrum already has a specific meaning, so it would be more correct to use something like "subalgebra spectrum", but because we believe that this notion is very important and that the word spectrum reflects this concept very well we use the word "spectrum". This makes our article more readable and in our context the interpretation should be unambiguous.

We have already seen in Theorem 3 how the spectrum naturally arises in the description of subalgebras of codimension one.

One trivial but useful remark is the following.

Theorem 5 *If $A \subseteq B$ are two subalgebras in $\mathbb{K}[x]$ then $Sp(B) \subseteq Sp(A)$. Thus the spectrum has the reversing inclusions property.*

Proof Each condition that holds in B holds in A as well. □

Theorem 6 *Each proper subalgebra A in $\mathbb{K}[x]$ has non-empty spectrum.*

Proof Induction and Theorem 4 shows that A is a subalgebra of a subalgebra of codimension 1. Then Theorems 5 and 3 finish the proof. □

While this theorem is valid for any proper subalgebra in $\mathbb{K}[x]$, it is shown in Sect. 27 that for polynomials in two variables one can find a proper subalgebra with empty spectrum.

One of our main results can be formulated as follows.

Theorem 7 *If A is a proper subalgebra of finite codimension then only the values of $f(x)$ and finitely many of its derivatives $f^{(j)}(x)$ in the elements of the spectrum determine if $f(x) \in A$.*

We will prove this later. We already have done so for monomial subalgebras and for subalgebras of codimension one.

Before moving on we give some equivalent definitions of the spectrum.

Theorem 8 *Let A be a subalgebra of finite codimension and $\alpha \in \mathbb{K}$. The following is equivalent.*

(i) *α belongs to the spectrum of A.*
(ii) *There exists $\beta \in \mathbb{K}$ such that $(x-\alpha)(x-\beta)$ divides $f(x)-f(\alpha)$ for any $f(x) \in A$.*
(iii) *There exists $\beta \in \mathbb{K}$ and a SAGBI basis G of A such that $(x-\alpha)(x-\beta)$ divides each element in G.*
(iv) *α belongs to the spectrum of the subalgebra $\langle p(x), q(x)\rangle$ for each pair of monic $p(x), q(x) \in A$ with relatively prime degrees.*

Note that the condition of relatively prime degrees in (iv) is necessary since it guarantees that $\langle p(x), q(x)\rangle$ is of finite codimension.

Proof (ii) is a simple reformulation of (i). (Note that we can take $\beta = \alpha$ when the condition is $f'(\alpha) = 0$).

(ii) implies (iii) almost directly. We choose any SAGBI basis and replace each element g by $g - g(\alpha)$ obtaining a new SAGBI basis.

(iii) implies (ii) because any $f(x) \in A$ can be subduced to a constant c. In each subduction step a polynomial divisible by $(x-\alpha)(x-\beta)$ is subtracted. Hence $f(x) - c$ is divisible by $(x-\alpha)(x-\beta)$. It is easy to see that we must have $c = f(\alpha)$.

By Theorem 5 (i) implies (iv). The opposite, that (iv) implies (i) is more difficult. If there exists $f(x) \in A$ such that $f'(\alpha) \neq 0$ we need to find β. Subtracting a constant we can suppose that $f(\alpha) = 0$ and let $\beta_1, \ldots, \beta_k$ be the other roots of $f(x)$, which exist because A is a proper subalgebra and $\mathbb{K}$ is algebraically closed. Then β should equal some β_i. If the implication does not hold then for each i there exists $g_i(x) \in A$ such that $g_i(\beta_i) \neq g_i(\alpha)$. Subtracting a constant we can suppose that $g_i(\alpha) = 0$, but $g_i(\beta_i) \neq 0$. Now, using that our field is infinite, we can easily construct a linear combination $g(x)$ of the g_i, such that $g(\alpha) = 0$ but $g(\beta_i) \neq 0$ for each i. Since A has a finite codimension we can for each large degree find a polynomial that belongs to A. We choose such a monic polynomial $h(x)$ that has degree larger than $\deg g(x)$ and relatively prime to $\deg f(x)$. We can also suppose that $h(\alpha) = 0$.

The next step is to construct a polynomial $p(x) = h(x) + cg(x)$ that has the same property as $g(x)$, namely $p(\alpha) = 0$ but $p(\beta_i) \neq 0$ for each i. Again, this is possible because our field is infinite. Let $q(x)$ be $f(x)$ divided by its leading coefficient. Consider the subalgebra $\langle p(x), q(x) \rangle$. Because α belongs to its spectrum and $q'(\alpha) \neq 0$ there exists β such that $p(\alpha) = p(\beta)$ and $q(\alpha) = q(\beta)$. But $q(\alpha) = 0$ so $\beta = \beta_i$ for some i. On the other hand $0 = p(\alpha) \neq p(\beta_i)$ and we get a contradiction. This proves that our assumption that (iv) does not imply (i) must have been wrong. □

8 Linear independence

To be sure that the maps we use later are linearly independent we need to prove some auxiliary statements, even though they may seem quite obvious or well-known.

Theorem 9 *Let $\alpha_1, \ldots \alpha_m$ be different elements in $\mathbb{K}$. The maps $L_{ij} : \mathbb{K}[x] \to \mathbb{K}$ defined by*

$$L_{ij}(f) = f^{(i)}(\alpha_j)$$

are linearly independent.

Proof Suppose the opposite. Then

$$\sum c_{ij} L_{ij} = 0$$

and WLOG $c_{k1} \neq 0$ and $c_{i1} = 0$ for $i > k$. Choose N such that $c_{ij} = 0$ for $i \geq N$ and consider

$$f(x) = (x - \alpha_1)^k \cdot \Pi_{j>1} (x - \alpha_j)^{(N+1)}.$$

Then $L_{ij}(f) = 0$ for $j > 1$ and for $j = 1, i < k$. On the other hand

$$L_{k1}(f) = k! \cdot \Pi_{j>1} (\alpha_1 - \alpha_j)^{(N+1)} \neq 0$$

and we get a contradiction. □

Naturally we can have some dependencies in a proper subalgebra but we want to show that all of them are linear combinations of defining subalgebra conditions.

Theorem 10 *Let V be a vector space over $\mathbb{K}$ and $L_1, \dots L_n$ be linear independent linear maps $L_i : V \to \mathbb{K}$. Consider the vector subspace $A = \bigcap_{i=1}^{n} \ker L_i$. Consider another linear map $l : V \to \mathbb{K}$ such that $l|_A = 0$. Then $l = \sum_{i=1}^{n} c_i L_i$ for some $c_i \in \mathbb{K}$.*

Proof We use induction on n. If $n = 1$ then $L_1 \neq 0$ and we can choose a vector $v \in V$ such that $L_1 v = 1$. Then $V = \mathbb{K}v + \ker L_1$ and because $\ker L_1 \subseteq \ker l$ we get that $l = c_1 L_1$, where $c_1 = l(v)$.

Now let $n > 1$. Consider $U = \bigcap_{i=2}^{n} \ker L_i$. Then by induction $L_1|_U \neq 0$ (otherwise the $L_i's$ are linearly dependent). Then $A = U \bigcap \ker L_1$ and the arguments above shows that $l|_U = c_1 L_1|_U$. Applying the induction to $l - c_1 L_1$ considered on U we get that $l - c_1 L_1 = \sum_{i=2}^{n} c_i L_i$ and we are done. □

9 The size of the spectrum

How large can the spectrum of a subalgebra of finite codimension n be? To answer this question we first prove an important statement, which essentially says that elements in the spectrum appear in a natural way and there are no "ghost" elements in the spectrum.

Theorem 11 *Suppose that the subalgebra A is obtained from the subalgebra B by adding an extra condition $L(f(x)) = 0$ where either $L(f(x)) = f(\alpha) - f(\beta)$ or L is some α-derivation. If $\lambda \notin Sp(B) \cup \{\alpha, \beta\}$ then $\lambda \notin Sp(A)$.*

Proof Suppose the opposite, that $\lambda \in Sp(A)$, but $\lambda \notin Sp(B) \cup \{\alpha, \beta\}$. Then for any $f = f(x) \in A$ we have $l(f) = 0$, where either $l(f) = f(\lambda) - f(\mu)$ or $l(f) = f'(\lambda)$. By Theorem 10 we get that $l = cL$ which obviously leads to the contradiction with Theorems 9 and 10 in all four different situations (two alternatives for L and two alternatives for l). □

Now we can get a bound for the size of the spectrum.

Theorem 12 *Let A be a subalgebra in $\mathbb{K}[x]$ of codimension n. Then*

- $|Sp(A)| \leq 2n$.
- $|Sp(A)| = 2n$ *if and only if A can be described by n conditions of the form $f(\alpha_i) = f(\beta_i), i = 1, \dots, n$, all $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ being different.*
- $|Sp(A)| = 2n - 1$ *if and only if A can be described by $n - 1$ conditions of the form $f(\alpha_i) = f(\beta_i), i = 1, \dots, n - 1$ and one extra condition either of the form $f'(\alpha_0) = 0$ or of the form $f(\alpha_0) = f(\alpha_1)$, all $\alpha_0, \dots, \alpha_{n-1}, \beta_1, \dots, \beta_{n-1}$ being different. The second alternative is possible only if $n > 1$.*

Proof The first two statements follow directly by induction from the previous theorem and Theorem 4. For the last statement we need to describe the induction in greater detail. For $n = 1$ the statement is trivial. If $n > 1$ and A is obtained from B by an extra condition then $|Sp(B)| \geq 2n - 3$. If $|Sp(B)| = 2n - 3$ the extra condition is of the form $f(\alpha) = f(\beta)$, where α, β does not belong to the spectrum of B and we can simply use the induction hypothesis. If $|Sp(B)| > 2n - 3$ then by Theorem 11 it must be $2n - 2$. If the extra condition is of the form $f(\alpha) = f(\beta)$ exactly one of α or β should belong to the spectrum of B. WLOG it coincides with α_1. Otherwise the extra condition is an α-derivation for some α that does not belong to $Sp(B)$. By Theorem 18 below we can replace it by $f(x) \to f'(\alpha)$ and it remains to rename α to α_0. □

10 The characteristic polynomial for subalgebras on two generators

Now we want to understand how to find the spectrum. We start from a special case where we can explicitly construct a polynomial which roots are exactly the elements of the spectrum.

Let $p(x)$, $q(x)$ be two monic polynomials. Consider the following polynomials in two variables:

$$P(x, y) = \frac{p(x) - p(y)}{x - y}, \; Q(x, y) = \frac{q(x) - q(y)}{x - y}.$$

We now introduce a definition that will be helpful when determining the spectrum of the subalgebra generated by p and q.

Definition 3 The **characteristic polynomial** $\chi_{p,q}$ is the resultant

$$\chi_{p,q}(x) = Res_y(P(x, y), Q(x, y))$$

of polynomials P and Q considered as polynomials in y.

For example, if $p(x) = x^3 - x, q(x) = x^2$ then $P(x, y) = y^2 + yx + x^2 - 1, Q(x, y) = y + x$ and

$$\chi_{p,q}(x) = \begin{vmatrix} 1 & x & x^2 - 1 \\ 1 & x & 0 \\ 0 & 1 & x \end{vmatrix} = x^2 - 1.$$

Its roots are 1 and -1 and this gives some insight into why $f(1) = f(-1)$ was the subalgebra condition for $A = \langle x^3 - x, x^2 \rangle$.

It is easy to check that get $\chi_{x^3,x^2}(x) = x^2$ and this can be easily generalised, as shown below.

Theorem 13 *If* $(m, n) = 1$ *then* $\chi_{x^n,x^m}(x) = x^{(n-1)(m-1)}$.

Proof Assume without loss of generality that $n > m$. First note that the polynomials $P(x,y) = \frac{x^n - y^n}{x-y}$ and $Q(x,y) = \frac{x^m - y^m}{x-y}$ can be expressed as $P = \sum_{i=0}^{n-1} y^i x^{n-1-i}$, $Q = \sum_{i=0}^{m-1} y^i x^{m-1-i}$ respectively. This means that

$$\chi_{p,q}(x) = \begin{vmatrix} 1 & x & \dots & x^{n-1} & 0 & 0 & \dots \\ 0 & 1 & \dots & x^{n-2} & x^{n-1} & 0 & \dots \\ \vdots & \ddots & & \ddots & \ddots & \ddots & \\ 0 & \dots & \dots & 1 & x & \dots & x^{n-1} \\ 1 & x & \dots & x^{m-1} & 0 & 0 & \dots \\ 0 & 1 & \dots & x^{m-2} & x^{m-1} & 0 & \dots \\ \vdots & \ddots & & \ddots & \ddots & \ddots & \\ 0 & \dots & \dots & 1 & x & \dots & x^{m-1} \end{vmatrix}.$$

If $m = 1$, this determinant is upper triangular and equal to $1 = x^{(m-1)(n-1)}$. This will be the base case for a proof by induction. If $m \neq 1$, for $i \in \{1, \dots, m-1\}$ we subtract row $m - 1 + i$ from row i. Now rows $1, \dots, m-1$ will have x^m as first nonzero element, in column $m + i$. One can break out a factor x^m from each of these rows. Now $\chi_A(x)$ is a block determinant on the form

$$\begin{vmatrix} 0 & B \\ A & C \end{vmatrix}$$

where A is an upper triangular $(m-1)$-matrix with ones on the main diagonal. Expanding the determinant along the first column $m - 1$ times and rearranging the rows gives

$$(x^m)^{m-1} \begin{vmatrix} 1 & x & \dots & x^{m-1} & 0 & 0 & \dots \\ 0 & 1 & \dots & x^{m-2} & x^{m-1} & 0 & \dots \\ \vdots & \ddots & & \ddots & \ddots & \ddots & \\ 0 & \dots & \dots & 1 & x & \dots & x^{m-1} \\ 1 & x & \dots & x^{n-m-1} & 0 & 0 & \dots \\ 0 & 1 & x & \dots & x^{n-m-1} & 0 & \dots \\ \vdots & \ddots & & \ddots & \ddots & \ddots & \\ 0 & \dots & \dots & 1 & x & \dots & x^{n-m-1} \end{vmatrix}$$

which is of size $(n-2)$. Note that this is exactly the characteristic polynomial of $\langle x^m, x^{n-m} \rangle$ multiplied by $(x^m)^{m-1}$.

Assuming, by induction hypothesis, that we have $\chi_{x^m, x^{n-m}}(x) = x^{(m-1)(n-m-1)}$ we get $\chi_{x^n, x^m}(x) = x^{m(m-1)} x^{(m-1)(n-m-1)} = x^{(m-1)(n-1)}$. The induction hypothesis can be used since $(n-m, m) = (n, m) = 1$. □

11 Computing $\chi_{p,q}$

An alternative proof of Theorem 13 stems from computing the resultant $\mathrm{Res}_y(P, Q)$ using reductions of P by Q and vice versa. A more exact statement is given in the below proposition. Here $lc(Q)$ denotes the leading coefficient of $Q(x, y)$ when regarded as a polynomial in y with coefficients in $\mathbb{K}[x]$, and degrees are also taken with respect to y.

Proposition 1 *Assume that $P, Q \in \mathbb{K}[x, y]$, and that $P_1(x, y) = P(x, y) - h(x, y)Q(x, y)$ for some polynomial $h \in \mathbb{K}[x, y]$. Then*

$$\mathrm{Res}_y(P, Q) = ((-1)^{deg(Q)} lc(Q))^{deg(P)-deg(P_1)} \mathrm{Res}_y\big(P_1, Q\big).$$

Similarly we have that

$$\mathrm{Res}_y(Q, P) = lc(Q)^{deg(P)-deg(P_1)} \mathrm{Res}_y\big(Q, P_1\big).$$

Proof This follows from the fact that the resultant

$$\mathrm{Res}_y(P, Q) = (-1)^{deg(P)deg(Q)} lc(Q)^{deg(P)} \prod P(x, \xi_i),$$

where ξ_i are the roots of Q when regarding Q as a polynomial in y. (See [5].) The roots are counted with multiplicity and they may lie in some extension of the field $\mathbb{K}[x]$ of coefficients.

Now, in the same way, we get an expression

$$\mathrm{Res}_y\big(P_1, Q\big) = (-1)^{deg(P_1)deg(Q)} lc(Q)^{deg(P_1)} \prod P_1(x, \xi_i),$$

but $P_1(x, \xi_i) = P(x, \xi_i) - h(x, \xi_i)Q(x, \xi_i) = P(x, \xi_i)$ and by comparing the two expressions we get the first statement of the proposition.

The second statement is proven in the same way, but is slightly easier to handle since $\mathrm{Res}_y(Q, P) = lc(Q)^{deg(P)} \prod P(x, \xi_i)$ does not contain powers of -1. □

The above proposition, which also can be found in [6], can be a useful tool for computing the characteristic polynomial when the generating polynomials are sparse. Let us first look at the two easy examples. We have

$$\begin{aligned}\chi_{x^2,x^3-x}(x) &= \mathrm{Res}_y\big(y + x, y^2 + xy + x^2 - 1\big) \\ &= \mathrm{Res}_y\big(y + x, x^2 - 1\big) = x^2 - 1\end{aligned}$$

and

$$\begin{aligned}\chi_{x^3,x^5}(x) &= \mathrm{Res}_y\big(y^2 + xy + x^2, y^4 + xy^3 + x^2y^2 + x^3y + x^4\big) \\ &= \mathrm{Res}_y\big(y^2 + xy + x^2, x^3y + x^4\big) = (x^3)^2 \mathrm{Res}_y\big(y^2 + xy + x^2, y + x\big) \\ &= x^6(y^2 + xy + x^2)|_{y=-x} = x^8.\end{aligned}$$

The second computation can be generalised to any case of two monomial generators, as follows. If $p = x^n$ and $q = x^m$ with $n = qm + r$ we can subtract powers of y

multiplied by Q from P until we obtain $P_1 = \sum_{j=0}^{r-1} x^{n-1-j}y^j = x^{n-r}\sum_{j=0}^{r-1} x^{r-1-j}y^j$. Note that the latter sum equals $H(x,y) = \frac{r(x)-r(y)}{x-y}$ for $h = x^r$. This can be used to obtain a more elegant inductive proof of Theorem 13 as

$$\begin{aligned}\chi_{p,q} &= \mathrm{Res}_y(P,Q) = (lc(Q)(-1)^{m-1})^{deg(P)-deg(P_1)}\mathrm{Res}_y\big(P_1,Q\big)\\ &= (lc(Q)(-1)^{m-1})^{qm}\mathrm{Res}_y(x^{n-r}H,Q) = (x^{n-r})^{m-1}\mathrm{Res}_y(H,Q) = (x^{n-r})^{m-1}\chi_{q,h}.\end{aligned}$$

By the induction hypothesis $\chi_{q,h} = x^{(m-1)(r-1)}$ and this results in

$$\chi_{p,q} = (x^{n-r})^{m-1}x^{(m-1)(r-1)} = (x^{n-1})^{m-1}$$

as we already knew from Theorem 13.

Finally, let us consider a more complicated example where we compute the characteristic polynomial of $A = \langle x^7 + 2x^3 - x, x^5 + x^2\rangle$.

Example 5 Let $p(x) = x^7 + 2x^3 - x$, $q(x) = x^5 + x^2$ and $P(x,y) = \frac{p(x)-p(y)}{x-y}$, $Q(x,y) = \frac{q(x)-q(y)}{x-y}$. Then

$$\chi_A(x) = \mathrm{Res}_y(P,Q) = \mathrm{Res}_y\big(P_1,Q\big)$$

where $P_1(x,y) = P(x,y) - y^2Q(x,y)$ is formed by subtracting multiples of Q from P in such a way that the y-degree decreases. Now $deg_y(P_1) = 3$ and $deg_y(Q) = 4$ so the next step is to form $Q_1(x,y) = Q(x,y) + (y+2)P_1(x,y) = a(x)y^2 + b(x)y + c(x)$. We have

$$\mathrm{Res}_y\big(P_1,Q\big) = lc(P_1)^2\mathrm{Res}_y\big(P_1,Q_1\big) = \mathrm{Res}_y\big(P_1,Q_1\big).$$

In the next step we want to reduce P_1 using Q_1, but Q_1 has a non-constant leading coefficient $a(x) = x^5 + x^2 + 4$. We can get around this problem as follows:

$$\begin{aligned}\mathrm{Res}_y\big(P_1,Q_1\big) &= \frac{1}{a^4}\mathrm{Res}_y\big(a^2P_1,Q_1\big)\\ &= \frac{1}{a^4}lc(Q_1)^2\mathrm{Res}_y\big(a^2P_1 + a(y-4)Q_1 + 8Q_1,Q_1\big)\\ &= \frac{1}{a^2}\mathrm{Res}_y\big(P_2,Q_1\big)\end{aligned}$$

where $deg_y(P_2) = 2$. A final step gives us $Q_2(x) = r(x)a(x)^2$. Here

$$\mathrm{Res}_y\big(P_2,Q_1\big) = \mathrm{Res}_y\big(P_2,Q_2\big) = Q_2,$$

and hence

$$r(x) = (x+1)^2(x^2-x+1)^3(x^3+x^2-x-2)^2h(x)$$

with $h(x) = (x^{10} - x^9 + 3x^8 - 3x^7 + 6x^6 - 2x^5 + 3x^4 - x^3 + x^2 + 3x - 2)$ is our desired resultant. This shows that Sp(A) has 16 elements. (One can verify that $h(x)$ has no multiple roots.)

As the above example shows, even if the process of computation is fairly simple, it is not easy to track how the resulting polynomial relates to the initial polynomials.

There are more efficient methods for computing resultants. For computing a resultant of two bivariate polynomials p, q of degree at most k there are well-know algorithms with time complexity $k^{3+o(1)}$. There are also more efficient algorithms known, see [7], but for our purposes standard implementations have been efficient enough.

12 Properties of $\chi_{p,q}$

Let us next turn to an interesting property of $\chi_{p,q}$. The below theorem relates $\chi_{p,q}$ to partial derivatives of a polynomial F that turns up when applying the standard algorithm for computing a SAGBI basis for $\langle p, q\rangle$. (See [1].) As we will see this theorem turns out to be an important building block for showing that derivations of non-spectral elements are trivial.

Theorem 14 *If* $m = \deg p(x), n = \deg q(x)$ *and* $(m, n) = 1$ *then*

- $\chi_{p,q}(x)$ *is a polynomial of degree* $(m-1)(n-1)$.
- *If* $F(p, q)$ *is the resultant of* $p(x) - p, q(x) - q$ *then*

$$\frac{\partial F}{\partial p}|_{p=p(x),q=q(x)} = \pm\chi_{p,q}(x)q'(x).$$
$$\frac{\partial F}{\partial q}|_{p=p(x),q=q(x)} = \mp\chi_{p,q}(x)p'(x).$$

Proof Let us look at what we did in the proof of Theorem 13 again. In a complete expansion of the determinant we choose in each column j either x^{j-i} (if we choose row i from the first $m-1$ rows) or we choose $x^{j-i+(m-1)}$ (if we choose a row i between the last $n-1$ rows). Because $\sum j = \sum i$ we get a total degree in the product equal to $(n-1)(m-1)$. We can never get larger degree. The difference when we use $p(x)$ and $q(x)$ instead is that we add some terms of smaller degree in each element of the matrix. But they cannot affect our maximum total degree term $x^{(n-1)(m-1)}$ so the highest coefficient in $\chi_{p,q}(x)$ at $x^{(n-1)(m-1)}$ is the same as for the monomial case.

To prove the second statement we use a well-known fact (see [8]) that

$$F(p, q) = \prod_{\alpha} p(\alpha) - p$$

where the product is taken over all roots of $q(y) - q$ in some field extension with multiplicity. When we evaluate this for $p = p(x)$ and $q = q(x)$ we get zero because $y = x$ is one of the roots. If we take a partial derivative with respect to p first and evaluate in $p = p(x)$ and $q = q(x)$ after that we get a sum over roots where all terms except one (corresponding the root $y = x$) are zero. But we can get this remaining

term in another way if we replace $q(x) - q$ by $\frac{q(y)-q(x)}{y-x}$ and $p(y) - p$ by $p(y) - p(x)$ in our resultant. Thus (up to sign) we get the resultant $\mathrm{Res}_y\left(p(y) - p(x), \frac{q(y)-q(x)}{y-x}\right)$.

Now, using another property of the resultant we get

$$\begin{aligned}
&\mathrm{Res}_y\left(p(y) - p(x), \frac{q(y) - q(x)}{y - x}\right) \\
&= \mathrm{Res}_y\left(\frac{p(y) - p(x)}{y - x}, \frac{q(y) - q(x)}{y - x}\right)\mathrm{Res}_y\left(y - x, \frac{q(y) - q(x)}{y - x}\right) \\
&= \chi_{p,q}(x)q'(x),
\end{aligned}$$

where all resultants above are evaluated in y. Here we have also used that for any polynomial $f(x)$ we have $f'(x) = \frac{f(x)-f(y)}{x-y}|_{y=x}$ because this is obviously true for $f(x) = x^k$. We obtain the second formula in a similar way and the signs should be opposite because $(F(p(x), q(x))' = F'_p p'(x) + F'_q q'(x)$ should be zero. □

Example 6 Let $p(x) = x^3 - x$, $q(x) = x^2$. Then $F(p, q)$ is the resultant of $x^3 - x - p$ and $x^2 - q$ and is equal to

$$F(p,q) = \begin{vmatrix} 1 & 0 & -1 & -p & 0 \\ 0 & 1 & 0 & -1 & -p \\ 1 & 0 & -q & 0 & 0 \\ 0 & 1 & 0 & -q & 0 \\ 0 & 0 & 1 & 0 & -q \end{vmatrix} = p^2 - q^3 + 2q^2 - q.$$

As expected we get:

$$\begin{aligned}
\frac{\partial F}{\partial p}|_{p=p(x),q=q(x)} &= 2p|_{p=p(x)} = 2(x^3 - x) = (x^2 - 1)2x, \\
\frac{\partial F}{\partial q}|_{p=p(x),q=q(x)} &= -3q^2 + 4q - 1_{p=p(x),q=q(x)} \\
&= -(q - 1)(3q - 1)_{p=p(x),q=q(x)} = -(x^2 - 1)(3x^2 - 1).
\end{aligned}$$

Are there instances when $\chi_{f,g}$ has an infinite number of roots? The answer is yes, as we have already seen for certain monomial subalgebras. More precisely we have seen that $\chi_{x^m,x^n} = 0$ if and only if $(m, n) > 1$. We will now generalise this result.

Theorem 15 *Let $p(x)$ and $q(x)$ be non-constant polynomials. Then $\chi_{p,q}(x) = 0$ if and only if there exists a polynomial $h(x)$ of degree at least two such that $p(x), q(x) \in \mathbb{K}[h]$.*

Proof Suppose first that $p = \pi \circ h$. We know $\pi(a) - \pi(b) = (a - b)\rho(a, b)$ for some ρ so

$$p(x) - p(y) = \pi(h(x)) - \pi(h(y)) = (h(x) - h(y))\rho(h(x), h(y)).$$

This means that $P(x,y) = \frac{p(x)-p(y)}{x-y}$ has a factor $\frac{h(x)-h(y)}{x-y}$ which is a polynomial in y of degree at least one. Similarly if $q(x) \in \mathbb{K}[h]$ then $Q(x, y)$ also has this factor so they have a common factor as polynomials in y over $\mathbb{K}(x)$ and as a consequence their resultant $\chi_{p,q}(x)$ is equal to zero.

To prove the opposite assume now that $\deg p(x) = n$ and $\deg q(x) = m$. Let $F(p, q)$ be the resultant of $p(x) - p, q(x) - q$, as before. We know from lemma 19 in [1] that $F(p,q) = \sum_{in+jm \leq nm} c_{ij} p^i q^j$ where c_{ij} are constants in $\mathbb{K}$. Moreover, it follows from that lemma that p^m has non-zero coefficient and all other terms contain p to a power strictly lower than m. Assume now that $\chi_{p,q}(x) = 0$. Then it follows from Theorem 14 that we can differentiate F with respect to p and get another identity involving p and q. Regarding p as variable this identity is a polynomial of degree $m-1$ with coefficients in $\mathbb{K}(q)$, showing that adjoining p to the field $\mathbb{K}(q)$ is an extension of degree at most $m-1$. From Lemma 13 in [1] we get the first equality in $m = [\mathbb{K}(x) : \mathbb{K}(q)] = [\mathbb{K}(x) : \mathbb{K}(p,q)][\mathbb{K}(p,q) : \mathbb{K}(q)]$. Now it follows that $[\mathbb{K}(x) : \mathbb{K}(p,q)] \geq 2$. On the other hand we know by Theorem 14 in [1] that $\mathbb{K}(p,q) = \mathbb{K}(h)$ for some polynomial h and this means that we have a polynomial h of degree $[\mathbb{K}(x) : \mathbb{K}(p,q)] \geq 2$ such that $p(x), q(x) \in \mathbb{K}[h]$. □

13 How the spectrum relates to $\chi_{p,q}(x)$

Now we want to compare the roots of the characteristic polynomial with the spectrum.

To start with we will focus our attention on a special case - an algebra A generated by two monic polynomials $p(x)$, $q(x)$ of degrees $m > n$ with $(m,n) = 1$. It is known that they form SAGBI basis for A (see [1]) and therefore A has codimension $g(m,n) = (m-1)(n-1)/2$. (Here $g(m, n)$ is the genus of the corresponding semigroup of degrees.) So if we want to describe this algebra we need to find $g(m, n)$ subalgebra conditions. For $m = 3, n = 2$ we have done that in Theorem 3.

Theorem 16 *Let $A = \langle p(x), q(x) \rangle$ and $\alpha \in \mathbb{K}$. The following* is equivalent.

(i) *α belongs to the spectrum, thus either $f'(\alpha) = 0$ for any $f(x) \in A$ or there exists $\beta \neq \alpha$ such that $f(\alpha) = f(\beta)$ for any $f(x) \in A$.*
(ii) *Either $p'(\alpha) = q'(\alpha) = 0$ or there exists $\beta \neq \alpha$ such that $p(\alpha) = p(\beta)$ and $q(\alpha) = q(\beta)$.*
(iii) *α is a root of the* characteristic polynomial *of A.*

Proof The alternatives (i) and (ii) are equivalent since each of the two conditions stated in (ii) are closed under sums and products, so we need only to prove that (ii) and (iii) are equivalent. By the fundamental property of the resultant (see e.g. [8]) we know that α is a root of the characteristic polynomial if and only if there is some $\beta \in \mathbb{K}$ such that $P(\alpha, \beta) = Q(\alpha, \beta) = 0$.

We now regard two different cases. The first case is when $\beta \neq \alpha$. In this case we have that $p(\alpha) - p(\beta) = (\alpha - \beta)P(\alpha, \beta) = 0$ and similarly $q(\alpha) = q(\beta)$. Thus the second statement of (ii) holds.

The other case is that $\alpha = \beta$ which means that $0 = P(\alpha, \alpha) = p'(\alpha)$. (The second equality can easily be derived from the definition of P as $P(x, y) = (p(x) - p(y))/(x - y)$.) In the same manner we find that $q'(\alpha) = 0$ so in this case the first statement of (ii) holds. □

This shows that the characteristic polynomial allows us to find the spectrum explicitly, for the subalgebras we currently study. Note that the theorem also shows that the characteristic polynomial is never a constant, because the spectrum is always non-empty.

Also note that Theorem 8 gives us a theoretical way to find the spectrum for any subalgebra. In most practical cases it is sufficient to consider only $\chi_{p,q}$ for each pair $\{p, q\}$ of generators, but the problem is that their degrees are not always relatively prime.

Here is another application of the theorem.

Proposition 2 *If $a(x)$ is a polynomial of degree at least two that divides both $p(x)$ and $q(x)$ then all the roots of $a(x)$ are roots of $\chi_{p,q}(x)$.*

Proof If $(x - \alpha)(x - \beta)|a(x)$ then $(x - \alpha)(x - \beta)|f(x) - f(\alpha)$ for any $f(x) \in A$ because p and q generate A and are divisible by $a(x)$. The rest follows from Theorems 8 and 16 . □

This shows that common factors of p and q with no multiple roots are also factors of $\chi_{p,q}$. By modifying the proof a little we can get the same result also for factors with multiple roots.

Theorem 17 *If $a(x)$ is a polynomial of degree at least two that divides both $p(x)$ and $q(x)$ then $a(x)|\chi_{p,q}(x)$.*

Proof Assume that $p(x) = a(x)p_1(x)$ and $q(x) = a(x)q_1(x)$. Now we modify $a(x)$ to separate its roots by introducing an additional variable s. If $a(x) = \prod_{i=1}^{k}(x - \xi_i)^{m_i}$, then let $\tilde{a} = \prod_{i=1}^{k}\prod_{l=1}^{m_i}(x - \xi_i - (l-1)s)$. Let $\tilde{p} = \tilde{a}p_1$ and $\tilde{q} = \tilde{a}q_1$. It follows that $\tilde{P}(x, y) = P(x, y) + sR(x, y)$ and $\tilde{Q}(x, y) = Q(x, y) + sT(x, y)$ for some polynomials R, T with coefficients in $k[s]$. Thus

$$\begin{aligned}\chi_{\tilde{P},\tilde{Q}}(x) &= Res_y(P(x, y) + sR(x, y), Q(x, y) + sT(x, y)) \\ &= Res_y(P(x, y), Q(x, y)) + sh(x, s) = \chi_{P,Q} + sh(x, s)\end{aligned}$$

for some polynomial h. The first equality in the last row comes from the fact that when computing the resultant from its definition as a determinant, every term that has been added contains at least one factor s. Now $\chi_{\tilde{P},\tilde{Q}}(x)$ has a factor $\tilde{a}(x)$ by the previous theorem. That is $\chi_{P,Q} + sh(x, s) = \tilde{a}(x)u(x, s)$. Now let $s = 0$ to conclude the proof. □

As an example, let us apply the above theorem as a tool for finding conditions for the subalgebra $A = \langle x^4 - x^2, x^3 \rangle$.

We see that x^2 divides both generators so it should divide the characteristic polynomial as well. Thus zero is in the spectrum. Moreover $f'(0) = 0$ is valid for both generators and therefore is one of the conditions. Because $g(4, 3) = 3$ we should find two additional subalgebra conditions. The characteristic polynomial can be found using Maple and it is equal to $x^2(x^4 - x^2 + 1)$.

Thus, besides zero we have four other elements in the spectrum, which are in fact primitive roots of degree 12. If we name one of them ε, the remaining ones will be $\varepsilon^5, \varepsilon^7, \varepsilon^{11}$. From Theorem 12 we find that the remaining conditions are of equality type. Thus we need to arrange those primitive roots in pairs to get conditions of the form $f(\alpha) = f(\beta)$. It is not hard to check that $\{f(x) | f'(0) = 0, f(\varepsilon) = f(\varepsilon^5), f(\varepsilon^7) = f(\varepsilon^{11})\}$ is the choice that contains x^3.

In fact, experiments suggests that when the degree of the factor $a(x)$ is higher than two its multiplicity as a factor of the resultant is higher.

Conjecture 1 If $a(x)$ is a polynomial of degree at least two that divides both $p(x)$ and $q(x)$ then $a(x)^{deg(a)-1} | \chi_{p,q}(x)$.

14 Derivations in *A*

Now we want to formulate some general statements about derivations. We begin our study with a subalgebra A, generated by two polynomials $p(x)$ and $q(x)$ of relatively prime degrees. As we know (see [1]) $p(x)$, $q(x)$ form a SAGBI basis and has one relation $F(p, q) = 0$ arising from the corresponding resultant. (Thus this F is the same as in theorem 14.)

Denote $D(p(x)) = Dp$ and $D(p(x)) = Dq$. First note that for any polynomial $G(p, q)$ we have

$$D(G(p(x), q(x)) = \frac{\partial G}{\partial p}(p(\alpha), q(\alpha))Dp + \frac{\partial G}{\partial q}(p(\alpha), q(\alpha))Dq.$$

If we denote $\frac{\partial F}{\partial p}(p(\alpha), q(\alpha))$ by $F'_p(\alpha)$ and $\frac{\partial F}{\partial q}(p(\alpha), q(\alpha))$ by $F'_q(\alpha)$ then we get that

$$F'_p(\alpha)Dp + F'_q(\alpha)Dq = 0$$

is a necessary and sufficient condition for a linear map D to be a derivation of A.

Note also that taking the ordinary derivative in α we get

$$F'_p(\alpha)p'(\alpha) + F'_q(\alpha)q'(\alpha) = 0.$$

Suppose now that α does not belong to the spectrum $Sp(A)$. Then we know that the vector $v = \left(p'(\alpha), q'(\alpha)\right)$ is non-zero. Also, according to Theorem 16, we have $\chi_{p,q}(\alpha) \neq 0$. Now it follows from Theorem 14 that the vector $w = \left(F'_p(\alpha), F'_q(\alpha)\right) \neq (0, 0)$. As the above equalities show that both the non-zero vector $v = \left(p'(\alpha), q'(\alpha)\right)$ and the vector (Dp, Dq) are orthogonal to w, they must be parallel. This means that

$(Dp, Dq) = c\big(p'(\alpha), q'(\alpha)\big)$ and thus we simply have $D(f(x)) = cf'(\alpha)$. In other words, D is a trivial derivation.

Now we generalise this to an arbitrary subalgebra A.

Theorem 18 *Let A be an arbitrary subalgebra of finite codimension and D be an α-derivation on A. Suppose that α does not belong to the spectrum of A.* Then *D is a trivial derivation, $D(f(x)) = cf'(\alpha)$.*

Proof Let $f(x)$ be any polynomial in A. First we prove that if α is a double root of $f(x)$ then $D(f(x)) = 0$. Suppose the opposite. Let $\beta_1, \ldots, \beta_k$ be the other roots of $f(x)$. For each i there exists $g_i(x) \in A$ such that $g_i(\beta_i) \neq g_i(\alpha)$. Subtracting a constant we can suppose that $g_i(\alpha) = 0$, but $g_i(\beta_i) \neq 0$. Beside that there exists $g_0(x) \in A$ such that $g_0(\alpha) = 0$, but $g_0'(\alpha) \neq 0$ (all this because α does not belong to the spectrum). Now, using the fact that an algebraically closed field is infinite, we can easily construct a linear combination $g(x)$ of the g_i such that $g(\alpha) = 0$ but $g(\beta_i) \neq 0$ for each $i > 0$ and $g'(\alpha) \neq 0$. Since A has a finite codimension we can for each large degree find a polynomial of that degree that belongs to A. We choose such a monic polynomial $h(x)$ that has degree larger than $\deg g(x)$ and relatively prime to $\deg f(x)$. We can also suppose that $h(\alpha) = 0$.

Our next step is to a construct polynomial $p(x) = h(x) + cg(x)$ that has the same property as $g(x)$, namely $p(\alpha) = 0, p'(\alpha) \neq 0$ and $p(\beta_i) \neq 0$ for each $i > 0$. Again, this is possible because our field is infinite. Let $q(x)$ be $f(x)$ divided by its leading coefficient. Consider subalgebra $B = \langle p(x), q(x) \rangle$. By construction α does not belong to its spectrum, so according to our arguments before the theorem the restriction of D to B should be a trivial derivation therefore $D(f(x)) = cf'(\alpha) = 0$ which is a contradiction.

The rest is easy. Any polynomial in A can be written as a linear combination of $g_0(x)$, some constant and some polynomial $f(x)$ having α as double root. Therefore only the value of $g_0(x)$ determine the value of D, so it is sufficient to find c such that $D(g_0(x)) = cg_0'(\alpha)$. □

15 Clusters

Let us now introduce a natural equivalence. For a given algebra A we define $\alpha \sim \beta$ if and only if $f(\alpha) = f(\beta)$ is valid for all $f \in A$. Then the spectrum of the subalgebra A is a disjoint union of equivalency classes that we call **clusters.** If A is obtained from B by a linear condition $L(f) = 0$ then Theorem 11 gives us a simple connection between clusters in B and A.

If L is an α-derivation then the clusters are the same if $\alpha \in Sp(B)$ and $\{\alpha\}$ constitutes an additional cluster in A if $\alpha \notin Sp(B)$.

If $L(f) = f(\alpha) - f(\beta)$ there are several possibilities. If neither α nor β belongs to the spectrum of B then they together form a new cluster.

If exactly one of them (say α) belongs to the spectrum of B then we simply add β to the cluster containing α.

At last if both α and β belong to the spectrum of B then they should lie in different clusters and as a result those two clusters will be joined in A.

From now on we will use the notion $A(C) = \{f(x) | f(\alpha) = f(\beta) \text{ for all } \alpha, \beta \in C\}$ for the subalgebra defined by the fact that all its elements have the same value on the cluster C.

16 The main theorem

Now we want to prove Theorem 7. We begin with the following statement.

Theorem 19 *Let A be a proper subalgebra of $\mathbb{K}[x]$ with $Sp(A) = \{\alpha_1, \ldots, \alpha_s\}$ and let $\pi_A = (x - \alpha_1) \cdots (x - \alpha_s)$. Then there exists $N > 1$ such that $x^i \pi_A^N \in A$ for any $i \geq 0$.*

Proof We use induction on the codimension n. The base for the induction is guaranteed by Theorem 3 so let $n \geq 2$. Let A be obtained from B as the kernel of L. Let $C = Sp(B)$, $\pi_B = \prod_{\gamma \in C}(x - \gamma)$ and N_B be the number N for the subalgebra B existing by the induction hypothesis. We consider several different cases.

Suppose first that $L(p) = p(\alpha) - p(\beta)$. We put $N = N_B$.

If both $\alpha, \beta \in C$ then $\pi_A = \pi_B$. Because $N > 0$ we get that all $x^i \pi_A^N \in \ker L = A$ directly.

If neither α nor β belongs to the spectrum of B then $\pi_A = \pi_B(x - \alpha)(x - \beta)$. Note that $x^i \pi_A^N \in B$ and $x^i \pi_A^N \in \ker L = A$.

If only $\alpha \in C$ then $\pi_A = \pi_B(x - \beta)$ and again $x^i \pi_A^N \in \ker L = A$ directly.

If L is an α-derivation and $\alpha \notin C$ then, according to Theorem 18, $L(f) = cf'(\alpha)$. We have that $\pi_A = \pi_B(x - \alpha)$ and put $N = N_B$. Because $N \geq 2$ we get that the multiplicity of α is at least two and $x^i \pi_A^N \in \ker L = A$.

At last if L is an α-derivation and $\alpha \in C$ then $\pi_A = \pi_B$ and we put $N = 2N_B$. Then $x^i \pi_A^{N_B}, \pi_A^{N_B} \in B$ and

$$L\left(x^i \pi_A^N\right) = L\left(x^i \pi_A^{2N_B}\right) = L\left(x^i \pi_A^{N_B}\right) \pi_A(\alpha)^{N_B} + \alpha^i \pi_A(\alpha)^{N_B} L\left((\pi_A)^{N_B}\right) = 0.$$

In all cases we get that $x^i \pi_A^N \in \ker L = A$. □

Theorem 20 *Let A be a subalgebra of codimension $n > 1$ with $Sp(A) = \{\alpha_1, \ldots, \alpha_s\}$. Then there exists $N > 1$ such that A can be described by n conditions of the form*

$$\sum_{i=0}^{N-1} \sum_{j=1}^{s} c_{ij} p^{(i)}(\alpha_j) = 0.$$

Thus $p(x) \in A$ if and only if all n conditions are valid.

Proof We use the same notation as in Theorem 19. According to that theorem we have polynomials in A of each degree greater than $Ns - 1$. If we complete them to a

linear basis in A we get a set Q, consisting of exactly $Ns - n$ new polynomials q and we can suppose that $1 \in Q$. Consider the vector space V consisting of linear maps

$$D : p(x) \to \sum_{i=0}^{N-1} \sum_{j=1}^{s} c_{ij} p^{(i)}(\alpha_j).$$

We have that $\dim V = Ns$. Consider its subspace W of those maps that annihilate all $q \in Q$. The subspace W has dimension n (because the condition $D(q) = 0$ is a homogeneous linear equation on the set of the coefficients c_{ij}). We choose a basis in W consisting of n maps D and claim that the conditions $D(p) = 0$ for each D from this basis describes A. Indeed those conditions by construction describe exactly the subspace generated by $q \in Q$ in the subspace of all the polynomials of degree less than Ns. It remains to show that each $x^i \pi_A^N$ is annihilated by D.

Let D_0 be the map

$$D_0 : p(x) \to \sum_{j=1}^{s} c_{0j} p(\alpha_j).$$

Because $\pi_A(\alpha_j) = 0$ for each j we have that $D_0(x^i \pi_A^N) = 0$ and it is sufficient to consider $D_1 = D - D_0$ consisting of only the derivatives. D_1 annihilates all the elements of the form $x^i \pi_A^N$ because it has derivatives of degree at most $N - 1$ and the same is true for D.

Thus our conditions are valid on all basis elements in A and describe the vector space they generate, which is A. In other words the conditions that $E_i(p(x)) = 0$ for our basis elements $E_i \in W$ determine the subalgebra A. Note that this automatically implies that we get subalgebra conditions. □

In fact we can prove a stronger result. The subalgebra conditions are either of form $f(\alpha) = f(\beta)$ or derivations. For non-trivial derivations we can prove (see [9]):

Theorem 21 *If α belongs to the spectrum then each α-derivation D can be written as*

$$D(f) = \sum_{i=1}^{N} \sum_{\alpha_j \sim \alpha} c_{ij} f^{(i)}(\alpha_j),$$

thus using pure derivatives (of some order) in the elements of the cluster containing α.

17 One element in the spectrum

Now we want to show some applications of the spectrum. We start from the subalgebras which have only one element in the spectrum.

Theorem 22 *Let A be a subalgebra of codimension $k \geq 1$. The following statements are equivalent.*

1. *The spectrum of A consists of a single element α.*
2. *A contains two elements $(x-\alpha)^m, (x-\alpha)^n$ with $(m,n)=1$.*
3. *A is defined by k linearly independent conditions of the form $\sum_{i=1}^{N} c_i f^{(i)}(\alpha) = 0$ for some $N > 0$.*

Proof We can use induction on k. The base for the induction is guaranteed by Theorem 3. Let $k \geq 2$. Using the change of variable $\hat{x} = x - \alpha$ we can restrict ourself to the case $\alpha = 0$.

(1) $\Rightarrow$ (2). According to Theorem 4 the algebra A is obtained from B as a kernel of some linear map. This map should be 0-derivation D, otherwise we have more than one element in the spectrum. By Theorem 5, B should have zero spectrum and according to the induction hypothesis B contains some monomials x^m, x^n with $(m,n)=1$. Note that $m,n>1$ because B is a proper subalgebra. Using that $D(f^k) = kf^{k-1}(0)D(f)$ we find that the monomials $(x^m)^m = x^{m^2}$, $(x^n)^n = x^{n^2}$ belong to $\ker D = A$.

(2) $\Rightarrow$ (1). Because the subalgebra generated by x^m and x^n has spectrum zero, by Theorem 5 the spectrum of A cannot have any other elements than zero.

(1) $\Rightarrow$ (3) Follows from Theorem 20.

(3) $\Rightarrow$ (2) All the monomials x^m with $m > N$ satisfy the conditions. □

18 Subalgebras containing a polynomial of degree 2

Suppose that the subalgebra A contains a polynomial $q(x)$ of degree two. Two trivial cases are $A = \langle q(x) \rangle$ and $A = \mathbb{K}[x]$. In non-trivial cases we should have a polynomial $p(x)$ of odd degree $2l+1 \geq 3$. If we suppose that l is as small as possible then it is easy to see that $A = \langle p(x), q(x) \rangle$. Using variable substitution we can suppose that $q(x) = x^2$. Subtracting even terms we can WLOG suppose that $p(x)$ is an odd polynomial, thus

$$p(x) = a(x^2)x, \; q(x) = x^2$$

for some monic polynomial $a(x)$ of degree l. We want to show that the spectrum of A consists of the roots of $a(x^2)$. (In fact the characteristic polynomial is equal to $a(x^2)$, but that requires a longer proof.)

Indeed, if $q'(\alpha) = 0$ then $\alpha = 0$ and $p'(0) = 0$ implies $a(0) = 0$. If $q(\alpha) = q(\beta)$ for $\alpha \neq \beta$ then $\beta = -\alpha$ and $p(\alpha) = p(-\alpha) = -p(\alpha)$ implies $p(\alpha) = 0 \Rightarrow a(\alpha^2) = 0$.

Now we are ready for the general statement.

Theorem 23 *Any proper subalgebra A of finite codimension in $\mathbb{K}[x]$ containing a polynomial $q(x)$ of degree two has a spectrum consisting of g elements for some $g > 0$. The spectrum has $k = \left[\frac{g}{2}\right]$ pairs $\{\alpha_i, \beta_i\}$, $i = 1, \dots, k$ such that for each i the sum $\alpha_i + \beta_i$ has a constant value $2\alpha_0$ and (for odd g) one extra element, namely $\alpha_0 (= \beta_0)$. For each $0 \le i \le k$ there exists number $m_i \ge 0$ such that $f(x) \in A$ if and only if*

- $f^{(j)}(\alpha_i) = (-1)^j f^{(j)}(\beta_i)$ *for each* $0 < i \le k$ *and each* $0 \le j \le m_i$,
- $f^{(j)}(\alpha_0) = 0$, $j = 1, 3, \dots, 2m_0 - 1$ (*for odd g only*).

Vice versa, if an algebra satisfies such conditions, then it is generated by

$$(x - \alpha_0)^2,\ (x - \alpha_0)^{2m_0+1} \prod_{i \ge 1} (x - \alpha_i)^{m_i+1} (x - \beta_i)^{m_i+1}.$$

Proof Since the codimension is finite and the subalgebra is proper we can after substitution suppose that A is generated by $p(x) = a(x^2)x$, $q(x) = x^2$, where $a(x)$ is a monic polynomial of degree $l > 0$. Here we put $\alpha_0 = 0$ and for each non-zero root μ_i of $a(x)$ with $i = 1, \dots, k$ we can put $\alpha_i = \sqrt{\mu_i}$ and $\beta_i = -\alpha_i$. We define m_0 to be the multiplicity of zero as a zero of $a(x)$ and put $g = 2k$ if $m_0 = 0$ and $g = 2k + 1$ if $m_0 > 0$. Now $a(x) = x^{m_0} \prod (x - \mu_i)^{m_i+1}$ and

$$\begin{aligned} p(x) &= x^{2m_0+1} \prod (x^2 - \mu_i)^{m_i+1} \\ &= x^{2m_0+1} \prod (x - \alpha_i)^{m_i+1} (x - \beta_i)^{m_i+1}. \end{aligned}$$

As we already discussed above the spectrum has exactly g elements. To check the conditions note that they are trivial for x^2 and that

$$p^{(j)}(\alpha_i) = p^{(j)}(-\alpha_i) = 0$$

if $j \le m_i$ for $i > 0$. If $m_0 > 0$ then all the derivatives until $2m_0 + 1$ are zero as well. Therefore $p(x)$ and $q(x)$ satisfy the conditions and it is sufficient to check that if $f(x)$ and $g(x)$ satisfy the conditions the same is true for $f(x)g(x)$. We have

$$\begin{aligned} (f(x)g(x))^{(j)}(\alpha_i) &= \sum_{j_1 + j_2 = j} \binom{j}{i_1} f^{(j_1)}(\alpha_i) g^{(j_2)}(\alpha_i) \\ &= \sum_{j_1 + j_2 = j} \binom{j}{i_1} (-1)^{j_1} f^{(j_1)}(-\alpha_i)(-1)^{j_2} g^{(j_2)}(-\alpha_i) \end{aligned}$$

and get the desired property both for $i > 0$ and $i = 0$ (because if j is odd one of j_1, j_2 is odd as well). So A satisfies the conditions. Let us now turn to the opposite direction. Our proof shows that the conditions determine some subalgebra that contains A and we need to prove that it equals A. If not there should be some polynomial $f(x)$ which does not belong to A. Using subduction by $p(x)$ and $q(x)$ we can suppose that it has an odd degree less than the degree of $p(x)$ and has only odd powers, and thus $f(-x) = -f(x)$.

Note that for an odd function $f(x)$ we have

$$f^{(j)}(\beta_i) = f^{(j)}(-\alpha_i) = -(-1)^j f^{(j)}(\alpha_i).$$

We get the opposite sign compared to our conditions so all terms must be zero. Thus α_i and β_i have multiplicity at least $m_i + 1$ as zeroes of $f(x)$. Similarly the second condition gives us that the multiplicity of zero as a zero is at least $2m_0 + 1$. But then $f(x)$ cannot have degree less than the degree of $p(x)$.

It remains to understand how we get back to the general case by using variable substitution back. Obviously α_0 is the only root of the derivative in $q(x)$ and the spectrum is simply shifted by α_0. □

19 α-Derivations

Now we want to collect some general properties of the set $\mathscr{D}_\alpha^A$ of α-derivations. Let A be a subalgebra of finite codimension and $M_\alpha = \{f(x) \in A | f(\alpha) = 0\}$ be the corresponding maximal ideal in A.

Theorem 24 *Let $D : A \to \mathbb{K}$ be a linear map.*

1. *The following statements are equivalent*:
   - *$D \in \mathscr{D}_\alpha^A$, thus D is an α-derivation.*
   - *$D(1) = 0$ and $D(f^2) = 0$ for any $f \in M_\alpha$.*
2. $\dim \mathscr{D}_\alpha^A = \dim M_\alpha / M_\alpha^2$ *(We denote this number d_α^A.)*
3. *If $T(A) = (d_1, \ldots, d_s)$ then $d_\alpha^A \leq s$.*

Proof (1) Obviously any α-derivation has these properties so we need only to work in the opposite direction.

For any $f \in A$ we have that

$$f - f(\alpha) \in M_\alpha \Rightarrow D\big((f - f(\alpha))^2\big) = 0 \Rightarrow$$
$$D(f^2) - 2f(\alpha)D(f) + D(f(\alpha)^2) = 0 \Rightarrow D(f^2) = 2f(\alpha)D(f).$$

Now for any $f, g \in A$ we have:

$$2D(fg) = D\big((f+g)^2 - f^2 - g^2\big) = 2(f(\alpha) + g(\alpha))D(f+g)$$
$$- 2f(\alpha)D(f) - 2g(\alpha)D(g) = 2(f(\alpha)D(g) + g(\alpha)D(f)).$$

(2) If we pick any SAGBI basis in M_α and choose those g_i from it that form a basis modulo M_α^2 then D will be uniquely determined by the values of $D(g_i)$. On the other hand we get an α-derivation for any choice of such values if we extend to a linear mapping that vanishes on constants and M_α^2, by part (1). The values of D on the remaining elements in the SAGBI basis will be uniquely determined. This also

proves (3) as we can start from a SAGBI basis with s elements and then possibly remove some of them to obtain our basis for the space of derivations. □

The type $T(A) = (d_1, \dots, d_s)$ gives us an upper bound $d_\alpha \leq s$ and we have equality in the monomial case. Indeed it is easy to check that the maps $D_i : f \to f^{(d_i)}(0)$ form a linear basis for the set $\mathscr{D}_0^A$ of zero-derivations.

Now we consider the following chain of subalgebras that differ by one in codimension:

$$\langle x^4, x^6, x^9, x^{11} \rangle \supset \langle x^4, x^6, x^9 \rangle \supset \langle x^6, x^8, x^9, x^{10}, x^{13} \rangle.$$

We see that d_α can both decrease by one and increase by two.

20 Some applications

Now we want to show some applications of the spectrum. First of all the spectrum gives us a much clearer picture of the inclusion of one subalgebra in another.

For example, which subalgebras B of codimension 2 can contain the subalgebra $A = \langle x^4, x^3 \rangle$ of codimension 3? The subalgebra $A \subseteq B$ has an element of degree 3, which does not belong to the semigroup generated by 2 and 5 so the type of B cannot be $(2, 5)$, thus $T(B) = (3, 4, 5)$.

Also $Sp(A) = \{0\}$ implies that $Sp(B) = \{0\}$ and our only candidate for B in the classification obtained in Theorem 27 below is $s = 1$ with $\alpha = 0$. Using that $x^3 \in B$ we can specify the conditions from the Theorem further to $f'(0) = f''(0) = 0$ and hence B must be the monomial algebra $\langle x^3, x^4, x^5 \rangle$.

Another obvious application is finding the intersection of two subalgebras: we take the union of their spectra and the union of their conditions and we only need to check if there are any linear dependencies between the conditions.

For example we can easily spot the situations when the intersection of two subalgebras is a monomial subalgebra. Both should have zero spectrum and the conditions of the subalgebras should complete each other so that we obtain conditions of the form $f^{(j)}(0) = 0$.

We can go in the opposite direction as well: if we have two subalgebras A_1, A_2 we can easily construct the subalgebra they generate together. We take the intersection of the spectra and try to see which conditions remain. Let us take an example from [2]. Is $\langle x^3 - x, x^4, x^5 - 1 \rangle = \mathbb{K}[x]$?.

The subalgebra $\langle x^4, x^5 \rangle$ is monomial, so its spectrum is zero. But zero is not in the spectrum of the subalgebra $\langle x^4, x^3 - x \rangle$, so the intersection of their spectra is empty and we get $\mathbb{K}[x]$. The most important application is the possibility to construct SAGBI bases without having to invoke the standard algorithm based on subduction. We will expand on this aspect in the next section.

21 Constructing SAGBI bases

One useful thing we want to mention is that the inductive approach which we have used throughout the article also allows us to create SAGBI bases in A relatively easily. Namely, when we have a SAGBI basis G for B and get A by adding the condition $L(f) = 0$ we do the following to obtain a SAGBI basis of A. All elements of G that satisfy the extra condition $L(f) = 0$ will remain in the SAGBI basis. There must, however, be at least one element that does not satisfy the condition. Let us choose such a $g \in G$ of minimal degree d, thus $L(g) \neq 0$. Note that exactly this degree d should disappear from the numerical semigroup S of degrees. Thus we know the new semigroup $S_A = S \setminus \{d\}$ and can easily find the type $(s_1, \dots, s_m)$ of the subalgebra A. For each degree s_i we find a polynomial $h_i \in B$ and our new SAGBI basis consists of $f_i = L(g)h_i - L(h_i)g$. If we wish to make them monic we can just divide each f_i by its highest coefficient. In order to further simplify calculations we want the basis elements to be inside M_α, and there are several ways to do this. The simplest one is to replace $f_i(x)$ by $f_i(x) - f_i(\alpha)$, but a more efficient way is to choose h_i and g in M_α from the start. Sometimes it may be clever to choose a linear combination with the previous f_j to get as high a degree of the factor $x - \alpha$ as possible.

We summarize this as follows.

Theorem 25 Let G be a SAGBI basis for B chosen inside M_α^B. Let $g = g_i$ be an element of minimal degree in this basis that does not belong to A. Suppose WLOG that $L(g) = 1$ and $L(g_j) = 0$ for $j \neq i$ (which we can obtain replacing g_j by $g_j - L(g_j)g$).

- The set consisting of polynomials g_j, $h_j = gg_j - L(gg_j)g$ with $g_j \in G$, $j \neq i$ and two polynomials $f_k = g^k - L(g^k)g$ for $k = 2, 3$ forms a SAGBI basis for A inside M_α^A. (Not necessary a minimal one.)
- If A has type $(s_1, \dots, s_m)$ then to construct a minimal SAGBI basis one should for each $s = s_j$ find a polynomial $p_s \in B$ of degree s and take $p_s - L(p_s)g$. If all p_s are chosen inside M_α^B then the obtained SAGBI basis will be inside M_α^A.

Proof If $f(x) \in B$ then $L(f - L(f)g) = 0$, thus $f - L(f)g$ belongs to $A = \ker L$. This immediately proves the second statement because we get elements of degree s_i in A. To prove the first statement we need to find polynomials built up from our basis elements of each degree $d \neq \deg g$ occurring in B. We can express d as the degree of some $g^l u$ where u is a product of g_j, where $j \neq i$, but repetitions are allowed. Because each such g_j belongs to M_α^A the same is true for u, so suppose that $l > 0$. If $l \geq 2$ we can use $f_2^a f_3^b u$ where $l = 2a + 3b$ to get the degree d. At last if $l = 1$ and $u = g_j v$ for some g_j we can use $h_j v$. □

Now we want to prove another result, where we want show how to use SAGBI bases.

Theorem 26 Let B be a subalgebra of finite codimension such that α does not belong to its spectrum. If D is a non-zero α-derivation of an algebra B and $A = \ker D$, then all α-derivations of subalgebra A can be written as

$$f(x) \to af'''(\alpha) + bf''(\alpha).$$

Proof First we choose a SAGBI basis $\{g_i\}$ for B inside M_α^B. Let $g = g_i$ be an element of minimal degree in this basis that does not belong to A. Suppose WLOG that $D(g) = 1$. Subtracting $c_j g$ we can suppose that $D(g_j) = 0$ for all $j \neq i$. By Theorem 25 the set consisting of polynomials g_j, $h_j = gg_j - D(gg_j)g$ with $g_j \in G$, $j \neq i$ and two polynomials $f_k = g^k - D(g^k)g$ for $k = 2, 3$ forms a SAGBI basis for A inside M_α^A.

By Theorem 18 we can suppose that $D(f) = f'(\alpha)$ and $d_\alpha^B = 1$. Then $f \to f^{(k)}(\alpha)$ for $k = 2, 3$ are two derivations and it is sufficient to prove that they are linearly independent and that $d_\alpha^A \leq 2$.

The linear independence is obvious if we restrict those maps to g^2, g^3 only, so let us concentrate on the inequality.

Because $d_\alpha^B = 1$ we have that

$$M_\alpha^B = \mathbb{K}g + \left(M_\alpha^B\right)^2.$$

In particular for $j \neq i$ we have

$$g_j \in \left(M_\alpha^B\right)^2.$$

This can be seen as follows:

$$\begin{aligned} &g_j = cg + m,\ m \in \left(M_\alpha^B\right)^2 \Rightarrow \\ &0 = D(g_j) = c + D(m) = c + 0 \Rightarrow c = 0. \end{aligned}$$

Using the fact that $D(g^2) = D(g^3) = D(gg_j) = 0$ we get that M_α^A is generated by g^2, g^3, g_j, gg_j with $j \neq i$. Note that all those elements belong to $\left(M_\alpha^B\right)^2$. Since both $\left(M_\alpha^B\right)^2$ and M_α^A have codimension one in M_α^B we conclude that

$$M_\alpha^A = \left(M_\alpha^B\right)^2.$$

Next we want to study when products $p = \Pi g_j$ of at least two elements belong to $\left(M_\alpha^A\right)^2$. This depends on the number of factors g_j that equal $g = g_i$. If there is no factor g then $p \in \left(M_\alpha^A\right)^2$. This also holds if at least four factors equal g, because g^n with $n \geq 4$ can be written as a product of g^2 and g^3.

If $p = g^3 u$ or $p = g^2 u$ where u does not contain g, the only exception is $p = g^3$ and $p = g^2$, because otherwise $u \in M_\alpha^A$.

At last if $p = gu$ then $u = g_j v$ and the only exception is $p = gg_j$. In all other cases $p = (gg_j)v \in \left(M_\alpha^A\right)^2$.

Because the products Πg_j span $\left(M_\alpha^B\right)^2$ we conclude that

$$\left(M_\alpha^B\right)^2 \subseteq \mathbb{K}g^2 + \mathbb{K}g^3 + \sum_{j\neq i} \mathbb{K}gg_j + \left(M_\alpha^A\right)^2. \tag{1}$$

We know that $g_k \in \left(M_\alpha^B\right)^2$ for $k \neq i$. As a result

$$gg_k \in \mathbb{K}g^3 + \mathbb{K}g^4 + \sum_{j\neq i} \mathbb{K}g^2g_j + g\left(M_\alpha^A\right)^2.$$

Using the facts that $g^4 = (g^2)^2, (g^2)g_j \in \left(M_\alpha^A\right)^2$ and $gM_\alpha^A \subseteq M_\alpha^A$ we find that

$$gg_k \in \mathbb{K}g^3 + \left(M_\alpha^A\right)^2.$$

Applying this for $k = j$ in (1) we can improve this to

$$M_\alpha^A = \left(M_\alpha^B\right)^2 \subseteq \mathbb{K}g^2 + \mathbb{K}g^3 + \left(M_\alpha^A\right)^2.$$

From this it is clear that

$$d_\alpha^A = \dim M_\alpha^A/\left(M_\alpha^A\right)^2 \leq 2.$$

Thus the two α-derivations of A we have found earlier form a basis for $\mathscr{D}_\alpha^A$. □

22 SAGBI bases in codimension one

Let us see how to find SAGBI bases in subalgebras of codimension one. We start from $\mathbb{K}[x]$ (which has x as SAGBI basis and from which we can get A either by the condition $f'(\alpha) = 0$ or by the condition $f(\alpha) = f(\beta)$). We now get Theorem 3 without any effort thanks to Theorem 4.

Now we want to prepare for the next codimension and for this we need to find SAGBI bases and derivations for the different subalgebras of codimension one. We obviously have that $\mathscr{D}_\alpha$ contains $f''(\alpha), f'''(\alpha)$ in the first case and $f'(\alpha), f'(\beta)$ in the second case.

Because d_α and d_β are not greater than the number of generators, which equals two, we have found all nontrivial derivations.

Type (2, 3) is the only possible semigroup of degrees, so an easy way to construct a SAGBI basis is to use the second part of Theorem 25. We get

$$(x-\alpha)^2, (x-\alpha)^3$$

as the SAGBI basis for the first alternative, that is when L is a derivation. For the second alternative we can choose

$$(x-\alpha)(x-\beta); (x-\alpha)^2(x-\beta).$$

23 Subalgebras of codimension two

We now turn to subalgebras of codimension two. By Theorem 4 they can be obtained by applying one extra condition to a subalgebra B of codimension one. This means we need to study how those conditions look. In the case when the extra condition is $f(\alpha) = f(\beta)$ we simply add one or two elements to the spectrum and obtain the algebra A. This is an easy case. A more difficult case is when we need to describe a kernel of some derivation. But we already know the derivations in each of the two cases considered above. Thus we are prepared to make a classification of all codimension two subalgebras:

Theorem 27 Let A be a subalgebra of codimension two. Then it is either type (2, 5) or type (3, 4, 5). The spectrum contains $s \leq 4$ elements and depending on s we have the following possibilities:

s=1 $A = \{f(x) | f'(\alpha) = 0; af''(\alpha) + bf'''(\alpha) = 0\}$.

If $a = 0, b \neq 0$ then $T(A) = (2, 5)$ and if $a \neq 0$ then $T(A) = (3, 4, 5)$.

s=2 $A = \{f(x) | f(\alpha) = f(\beta); af'(\alpha) + bf'(\beta) = 0\}$.

If $a = b \neq 0$ then $T(A) = (2, 5)$ and if $a \neq b$ then $T(A) = (3, 4, 5)$.

s=2 $A = \{f(x) | f'(\alpha) = f'(\beta) = 0\}$.

In this case $T(A)$ is always (3, 4, 5).

s=3 $A = \{f(x) | f(\alpha) = f(\beta); f'(\gamma) = 0\}$.

If $\alpha + \beta = 2\gamma$ then $T(A) = (2, 5)$, and if $\alpha + \beta \neq 2\gamma$ then $T(A) = (3, 4, 5)$.

s=3 $A = \{f(x) | f(\alpha) = f(\beta) = f(\gamma)\}$.

In this case $T(A)$ is always (3, 4, 5).

s=4 $A = \{f(x) | f(\alpha) = f(\beta); f(\gamma) = f(\delta)\}$.

If $\alpha + \beta = \gamma + \delta$ then $T(A) = (2, 5)$ and if $\alpha + \beta \neq \gamma + \delta$ then $T(A) = (3, 4, 5)$.

Here $\alpha, \beta, \gamma, \delta$ are different elements of the spectrum.

Proof We know that the spectrum has at most four elements. We start with the case where there are no derivations in the subalgebra conditions. Either we have two clusters and get the only case with $s = 4$ or we have only one cluster of size 3 and get the second case with $s = 3$.

If some γ-derivation is used then we can suppose that it was added to a subalgebra of codimension one. If γ was not in the spectrum of this codimension one subalgebra, then γ is a trivial derivation $f \to f'(\gamma)$ and we get either the second case with $s = 2$ (with $\gamma = \beta$) or the first case with $s = 3$.

At last if γ belongs to the spectrum we can WLOG suppose that $\gamma = \alpha$ and use that we know all α-derivations. We get cases with $s = 1, 2$.

It is easy to check that (2, 5) and (3, 4, 5) are the only choices for the numerical semigroup of degrees. To see which choice is valid we only need to check if the element of degree 2 in the SAGBI basis satisfies the added condition. If so we get type (2, 5), otherwise type (3, 4, 5). Alternatively we can use Theorem 23 which tells us exactly when $T(A) = (2, 5)$. □

24 Subalgebras of codimension three

In codimension three we can use the same approach and get a classification, but the situation is more complicated. The spectrum has at most 6 elements. We will show only how it looks for a single element in the spectrum (the complete classification can be found in [10]).

Theorem 28 If an algebra A of codimension three has a spectrum consisting of a single element α then A is one of the following algebras

1. $A = \{f(x) | f'(\alpha) = f''(\alpha) = af'''(\alpha) + bf^{(4)}(\alpha) + cf^{(5)}(\alpha) = 0\}$.
   If $a \neq 0$ then $T(A) = (4, 5, 6, 7)$ and for $a = 1$ a SAGBI basis is:

   $$(x-\alpha)^4 - 4b(x-\alpha)^3, (x-\alpha)^5 - 20c(x-\alpha)^3, (x-\alpha)^6, (x-\alpha)^7.$$

   If $a = 0$ and $b \neq 0$ then $T(A) = (3, 5, 7)$ and for $b = 1$ a SAGBI basis is:

   $$(x-\alpha)^3, (x-\alpha)^5 - 5c(x-\alpha)^4, (x-\alpha)^7.$$

   For $a = b = 0, c \neq 0$ the type is (3, 4) and a SAGBI basis is

   $$(x-\alpha)^3, (x-\alpha)^4.$$

   If $a = b = c = d = 0$ the codimension is 2.
2. $A = \{f(x) | f'(\alpha) = f'''(\alpha) - 3af''(\alpha) = f^{(5)}(\alpha) - 10af^{(4)}(\alpha) + bf''(\alpha) = 0\}$.
   with $a \neq 0$. If $b \neq 0$ then $T(A) = (4, 5, 6, 7)$ and a SAGBI basis is:

   $$b(x-\alpha)^4 + 120a^2(x-\alpha)^3 + 120a(x-\alpha)^2,$$
   $$b(x-\alpha)^5 - 60a(x-\alpha)^3 - 60(x-\alpha)^2, (x-\alpha)^6, (x-\alpha)^7.$$

If $b = 0$ then $T(A) = (3, 5, 7)$ and a SAGBI basis is:

$$(x-\alpha)^3 + a(x-\alpha)^2, 2a(x-\alpha)^5 + (x-\alpha)^4, (x-\alpha)^7.$$

3. $A = \{f(x) | f'(\alpha) = f'''(\alpha) = cf^{(5)}(\alpha) + df''(\alpha) = 0\}$. If $d \neq 0$ then $T(A) = (4, 5, 6, 7)$ and a SAGBI basis is:

$$(x-\alpha)^4, d(x-\alpha)^5 - 60c(x-\alpha)^2, (x-\alpha)^6, (x-\alpha)^7.$$

If $c \neq 0, d = 0$ then $T(A) = (2, 7)$ and a SAGBI basis is:

$$(x-\alpha)^2, (x-\alpha)^7.$$

If $c = 0, d = 0$ we get codimension 2.

Proof The subalgebra A is contained in a subalgebra B of codimension 2. Because the spectrum of B is a subset of the spectrum of A, the subalgebra B should have a single (and the same) element α in the spectrum. Moreover, A is obtained from B as a kernel of some α-derivation (all other possibilities would lead to a larger spectrum). So the result will follow from the description of all derivations of the subalgebra $B = \{f(x) | f'(\alpha) = 0; a_1 f''(\alpha) + b_1 f'''(\alpha) = 0\}$ by adding an extra derivation. Using variable substitution $x - \alpha \to x$ we can WLOG suppose that $\alpha = 0$. If $a_1 = 0$ (which corresponds to $T(B) = (2, 5)$) we put $b_1 = 1$ and get a monomial subalgebra B, where we know all derivations and obtain case 3.

If $b_1 = 0$ we get a monomial subalgebra as well, and get the case 1. Otherwise we can put $b_1 = 1$, and (in order to get a nice SAGBI basis) $a_1 = -3a$ where we suppose that $a \neq 0$. Thus

$$f'''(0) - 3af''(0) = 0.$$

Because $T(B) = (3, 4, 5)$ we can choose $p = x^4, q = ax^3 + x^2, r = x^5$ as generators of B. Note that $a^2p^2 - aqr + pq = x^6 \in M_0^2$. Thus

$$q^2 - a^2x^6 = 2ax^5 + x^4 = 2ar + p \in M_0^2$$

and we get $2aDr + Dp = 0$. Therefore $d_0^B \leq 2$ which means that we only need to find two derivations of the desired form.

One is obviously the second derivative, $D_1 : f(x) \to f''(0)$, but we cannot use the third derivative because in our algebra it is proportional to D_1. So we need to try higher derivatives $D_2 : f(x) \to cf^{(4)}(0) + df^{(5)}(0)$. Our condition $2aD_2r + D_2p = 0$ is equivalent to $2a \cdot d \cdot 5! + c \cdot 4! = 0$ so we can try $c = -10a, d = 1$ and only have to check that this is a derivation in B. We have (skipping terms that obviously equal zero)

$$
\begin{aligned}
&- 10a(fg)^{(4)}(0) + (fg)^{(5)}(0) \\
&\quad - \big(-10af^{(4)}(0) + f^{(5)}(0)\big)g(0) - f(0)\big(-10ag^{(4)}(0) + g^{(5)}(0)\big) \\
&= -10a\binom{4}{2}f''(0)g''(0) + \binom{5}{2}f'''(0)g''(0) + \binom{5}{3}f''(0)g'''(0) \\
&= -10a \cdot 6f''(0)g''(0) + 10 \cdot 3af''(0)g''(0) + 10 \cdot 3af''(0)g''(0) = 0
\end{aligned}
$$

and we are done.

The arbitrary derivation is a linear combination of $f(x) \to f''(\alpha)$ and $f(x) \to f^{(5)}(\alpha) - 10af^{(4)}(\alpha)$ and we get the case 2 if we simply substitute 0 by α back.

When we get a description there is a straightforward way described above to get a SAGBI basis: we know the possible degrees and need only to search for elements of the degrees generating the semigroup that satisfy the subalgebra conditions. □

25 About the characteristic polynomial $\chi_A(x)$ when A has more than two generators

We would like to generalise Theorem 16 to arbitrary subalgebras. For this we need to define the characteristic polynomial for an arbitrary subalgebra.

Let us look at the case where A has more than two generators. It is not evident how to extend the definition. The resultant is defined only for pairs of polynomials.

A naive attempt is to use the gcd of all χ_{g_i,g_j} where g_i generate A. Let us first look at an example.

Example 7 Let $p(x) = x^{12} + 3x^6$, $q(x) = x^{15}$ and $r(x) = x^{10}$ and $A = \langle p(x), q(x), r(x)\rangle$ the subalgebra they generate. We can form the characteristic polynomial of any pair of generators. If we look at the pair p and q for example, it is obvious that they both belong to $\mathbb{K}[x^3]$. Hence their characteristic polynomial is zero by Theorem 15. In the same way the other two pairs of generators have zero as characteristic polynomial. In contrast, if we form P and Q as before and additionally $R(x, y) = (r(x) - r(y))/(x - y)$, then $P(x, y) = Q(x, y) = R(x, y) = 0$ has only a finite set of solutions. In particular the possible x-values are the 24 solutions of $x^{24} + 6x^{18} + 26x^{12} + 81x^6 + 81$ and $x = 0$. (This can be obtained by solving the system in for example Maple.)

The above example shows that looking at pairs of generators of the algebra is not enough to define the characteristic polynomial in a suitable way. Inspired by Theorem 8 we instead make the following definition.

Definition 4 Let A be a subalgebra of finite codimension. We define its **characteristic polynomial** $\chi_A(x)$ as the gcd of all $\chi_{p,q}(x)$ where p and q are monic polynomials in A with relatively prime degrees.

Theorem 8 assures that the set of zeroes of $\chi_A(x)$ equals the spectrum.

This definition has the drawback that it does not give an immediate way to compute $\chi_A(x)$, as there are infinitely many pairs $\{p, q\}$.

We will therefore introduce another polynomial, $D(x)$, that while still having the spectrum as its set of zeroes, also immediately allows computation for each finitely generated A.

Let us first assume that we have three generators $A = \langle p(x), q(x), r(x)\rangle$. We also assume that $\deg q(x) \geq \deg r(x)$. Introduce $P(x, y)$, $Q(x, y)$ as before and analogously $R(x, y)$. Then form the resultant $R(x, y, z) = \mathrm{Res}_y(P(x, y), zQ(x, y) + wR(x, y))$. An x-value $x = \alpha$ that makes this resultant disappear for all values of z and w means an x-value for which there is some $y = \beta$ such that $P(\alpha, \beta) = 0$ and $zQ(\alpha, \beta) + wR(\alpha, \beta) = 0$ regardless of the values of z and w. In other words $P(\alpha, \beta) = Q(\alpha, \beta) = R(\alpha, \beta) = 0$.

Now it follows, from the construction of the resultant as a certain determinant and the fact that the determinant depends linearly on the columns of the matrix, that R can be written as $R(x, z, w) = \sum_{j=0}^{n-1} d_j(x) z^{n-1-j} w^j$. Here $d_j(x)$ is a polynomial in $\mathbb{K}[x]$ that can be computed by starting from the resultant-matrix of P and Q, then replace j columns of coefficients from Q by the corresponding coefficients of R. Finally sum over all choices of j such column replacements. That sum of determinants equals $d_j(x)$. The x-values $x = \alpha$ that make $R(\alpha, z, w) = 0$ are those which satisfy $d_j(\alpha) = 0$ for each j or equivalently those $x = \alpha$ that are zeroes of $d(x) = gcd(d_1(x), d_2(x), \ldots, d_{n-1}(x))$. It is straightforward to generalise this idea to more than three generators. We therefore make the following definition:

Definition 5 Let $A = \langle p_1(x), p_2(x), \ldots, p_t(x)\rangle$ and $n = \deg p_1(x)$. Moreover, form $P_i(x, y) = (p_i(x) - p_i(y))/(x - y)$ and finally

$$\begin{aligned} &R(x, z_2, z_3, \ldots, z_t) \\ &\quad = \mathrm{Res}_y\big(P_1(x, y), z_2 P_2(x, y) + z_3 P_3(x, y) + \cdots + z_t P_t(x, y)\big). \end{aligned}$$

Then R can be expressed as

$$R(x, z_2, z_3, \ldots, z_t) = \sum d_{(a_2, a_3, \ldots, a_t)}(x) z_2^{a_2} z_3^{a_3} \cdots z_t^{a_t}, \tag{2}$$

where the sum is taken over all natural numbers a_i satisfying $a_2 + a_3 + \cdots a_t = n - 1$. Now let $D(x) = gcd(\{d_{(a_2, a_3, \ldots, a_t)}\})$ where the gcd is taken over the set of all polynomials $d_{(a_2, a_3, \ldots, a_t)}$ occurring in the sum (2).

This definition looks complicated, so let us see how it works in our previous example.

Example 8 Let p, q, r and P, Q, R be as in the previous example. In this case we need to compute the resultant

$$\mathrm{Res}_y(P(x, y), zQ(x, y) + wR(x, y)) = \sum_{j=0}^{10} d_{(10-j,j)}(x).$$

(Here we have replaced z_2 by z and z_3 by w to improve readability.) By doing our computation in Maple we obtain:

$$\begin{aligned} d_{(11,0)} &= d_{(10,1)} = 0 \\ d_{(9,2)} &= 4x^{60}a(x)^2b(x)^3 \\ d_{(8,3)} &= 18x^{55}a(x)b(x)^2c(x) \\ d_{(7,4)} &= 3x^{50}b(x)d(x) \end{aligned}$$

where

$$\begin{aligned} a(x) = 2x^6 + 3, b(x) = x^{24} + 6x^{18} + 36x^{12} + 81x^6 + 81, \\ c(x) = 2x^{30} + 5x^{24} + 30x^{18} + 90x^{12} + 135x^6 + 81 \end{aligned}$$

and

$$\begin{aligned} d(x) = 52x^{60} + 300x^{54} + 2025x^{48} + 8100x^{42} + 24300x^{36} + 65610x^{30} \\ + 153090x^{24} + 262440x^{18} + 295245x^{12} + 196830x^6 + 59049. \end{aligned}$$

Thus the gcd of the first five polynomials $d_{(11-j,j)}$ is $x^{50}b(x)$. One can check that the remaining $d_{(11-j,j)}$ also are divisible by $x^{50}b(x)$. (In particular $d_{(0,11)} = 0$, while the other polynomials are non-zero.)

Thus $D(x) = x^{50}b(x)$, and the $Sp(A)$ consists of zero together with the 24 zeroes of $b(x)$.

Note that $D(x)$ depends on the generators and even on which generator is chosen as p_1. For example if we take $p_1 = r$ in the above example we get $D(x) = x^{54}b(x)$. As long as we are looking for the zeroes this is not a problem, but we cannot use D as our characteristic polynomial as it is not well defined for a given subalgebra A.

But we can define characteristic polynomial as a gcd of all such $D(x)$ to have an invariant definition. In our example it still be $x^{50}b(x)$.

We conclude by using D to find descriptions of some subalgebras on several generators.

Example 9 Let

$$A = \langle (x-5)(x-4)(x-2)(x-1)x^3, (x-5)(x-4)(x-2)(x-1)x, (x-5)(x-4)x \rangle.$$

Using the above method we get $D(x) = x^2(x-1)(x-2)(x-4)^2(x-5)^2$. Hence $Sp(A) = \{0, 1, 2, 4, 5\}$. Since A has generators of degrees 3, 5, 7 its codimension in $\mathbb{K}[x]$ is at most three. By Theorem 7 we should look for conditions where f or its derivatives are evaluated in spectral points. It is evident that $f(0) = f(4) = f(5)$ for all generators. Also $f(1) = f(2)$ for the first two generators, and one can check that this holds also for the third generator. This shows that $A = \{f(x) | f(0) = f(4) = f(5), f(1) = f(2)\}$. Note that since we found three conditions the codimension equals three, and this implies that our generators constitute a SAGBI basis.

Example 10 Let

$$A = \langle x^4 - x^2 + 4, x^5 - 5x^3 + 4x, x^6 - 5x^4 + 4x^2, x^7 - 5x^5 + 4x^3 \rangle.$$

In this case we get $D(x) = x^2(x-2)(x+2)(x-1)^2(x+1)^2$. Thus we get that $Sp(A) = \{0, 1, -1, 2, -2\}$. Since A has generators of degrees 4, 5, 6, 7 we must again have codimension at most three. If we factor the generators it is easy to see that $A = \{f(x) | f(0) = f(1) = f(-1), f(2) = f(-2)\}$.

Finally we want to consider quite different approach to generalise the notion of characteristic polynomial for to an arbitrary subalgebra A. It is based on the observation that the characteristic polynomial belongs to the subalgebra itself. According to Theorem 19 there exists a monic polynomial $p(x)$ such that $x^k p(x) \in A$ for any $k \geq 0$. If we choose such polynomial of minimal degree it will be unique. (Otherwise the difference between two such polynomials would provide a polynomial of lower degree.) Let us take call such a minimal polynomial $M(x)$.

Note that any $\alpha \in Sp(A)$ is a root for $M(x)$. This is immediate from the definition of spectrum applied to the elements $M(x)$ and $xM(x)$ of A. Obviously its degree is greater than the Frobenius number of the the corresponding numerical semigroup S of degrees. As we see in the last example it can be larger than the Frobenius number plus one, but we suspect it is not greater than twice the codimension. We have $M(x) = x^{30} b(x)$ in Example 8, so here the degree is exactly twice the codimension, but it is smaller than the degree of the characteristic polynomial obtained using our previous definition. It seems reasonable to think of $M(x)$ as a kind of minimal polynomial for A, but one could also take $M(x)$ to be the characteristic polynomial of A.

26 Single element in the spectrum: derivations

To understand how derivations are formed, we will study a special concrete case, algebras A with a single element α in the spectrum.

First of all, if $p'(\alpha) = 0$ for any $p \in A$, then $D_2 : p \to \frac{p''(\alpha)}{2!}$ and $D_3 : p \to \frac{p'''(\alpha)}{3!}$ are two α-derivations over A. Now one may ask: what α-derivations exist over the kernel of some linear combination $D_3 - cD_2$? Consider the following list of the maps created with the help of Maple:

$$
\begin{gathered}
D_1 \\
D_3 - cD_2; \\
D_5 - 2cD_4; \\
D_7 - 3cD_6 + 3c^3D_4; \\
D_9 - 4cD_8 + 11c^3D_6 - 11c^5D_4; \\
D_{11} - 5cD_{10} + 26c^3D_8 - 78c^5D_6 + 78c^7D_4; \\
D_{13} - 6cD_{12} + 50c^3D_{10} - 294c^5D_8 + 882c^7D_6 - 882c^9D_4; \\
D_{15} - 7cD_{14} + 85c^3D_{12} - 816c^5D_{10} + 4811cD_8^7 - 14433c^9D_6 + 14433c^{11}D_4; \\
D_{17} - 8cD_{16} + 133c^3D_{14} - 1881c^5D_{12} + 18145c^7D_{10} \\
- 106989c^9D_8 + 320967c^{11}D_6 - 320967c^{13}D_4; \\
D_{19} - 9cD_{18} + 196c^3D_{16} - 3822c^5D_{14} + 54399c^7D_{12} \\
- 524880c^9D_{10} + 3094881c^{11}D_8 - 9284643c^{13}D_6 + 9284643c^{15}D_4.
\end{gathered}
$$

Here D_k is the map $D_k : p \to \frac{p^{(k)}(\alpha)}{k!}$ and c is a constant.

We know that the first map is an α-derivation. But what is more interesting is that if the first k maps defines a subalgebra inside A (as the intersection C of their kernels with A), then the next map will be a derivation over C.

For any given map in the list above, let C_i be the coefficient of $c^k D_i$. I.e in the fourth map we have $C_7 = 1, C_6 = -3, C_4 = -3$. Then for every single map, the following relations all hold among the C_i of that map:

$$
\begin{gathered}
C_0 = 0 \\
C_2 + C_3 = 0; \\
C_4 + 2C_5 + C_6 = 0 \\
C_6 + 3C_7 + 3C_8 + C_9 = 0 \\
C_8 + 4C_9 + 6C_{10} + 4C_{11} + C_{12} = 0 \\
\cdots \\
C_{2m} + \binom{m}{1} C_{2m+1} + \binom{m}{2} C_{2m+2} + \cdots + \binom{m}{m-1} C_{3m-1} + C_{3m} = 0.
\end{gathered}
$$

We use parenthesised superscripts to index a particular map above. We index the maps by the highest order among the derivatives in it. Note that this means that the map with index n is in row $\frac{n+1}{2}$ in the above list. For example

$C_6^{(7)} = -3$. The following theorem states that the properties which we have observed (but not proved) the $C_k^{(n)}$ to exhibit, uniquely determine a set of integers.

Theorem 29 *Let $n = 2k + 1$ be an odd number. If we demand*

- $C_n^{(n)} = 1$ *and* $C_i^{(n)} = 0$ *for all other odd* i;
- $C_i^{(n)} = 0$ *for all even* $i > n$;
- $C_{2m}^{(n)} + \binom{m}{1} C_{2m+1}^{(n)} + \binom{m}{2} C_{2m+2}^{(n)} + \binom{m}{3} C_{2m+3}^{(n)} + \cdots + \binom{m}{m-1} C_{3m-1}^{(n)} + C_{3m} = 0$ *for all* m

then the numbers $C_i^{(n)}$ are uniquely determined.

Proof We only need to consider $C_i^{(n)}$ for even i less than n. For $C_{2k}^{(n)}$ we have

$$C_{2k}^{(n)} + \binom{k}{1} C_{2k+1} + 0 + \cdots = 0 \Rightarrow C_{2k}^{(n)} = -\binom{k}{1} = -k.$$

If $C_i^{(n)}$ is defined for all $i > 2m$ then we have

$$C_{2m}^{(n)} = -\left[\binom{m}{1} C_{2m+1}^{(n)} + \binom{m}{2} C_{2m+2}^{(n)} + \cdots + \binom{m}{m-1} C_{3m-1}^{(n)} + C_{3m}\right]$$

and all $C_i^{(n)}$ are uniquely defined by induction. □

Now for each odd n we can define

$$L_n = \sum_{i=0}^{n} C_i^{(n)} c^i D_{n-i}.$$

Conjecture 2 If $L_1(f) = L_3(f) = \cdots = L_{n-2}(f) = 0$ for each $f \in A$ then L_n is an α-derivation in A.

27 Further development

Here we want to discuss some possible ways to generalise the obtained results. We have several restrictions. Are they all necessary?

First of all we can consider subalgebras of infinite codimension. Then we need infinitely many conditions, so spectra can be infinite as well. But there are many interesting questions here.

Next we have the restrictions on the field. Characteristic zero seems to be important. In positive characteristic we encounter problems already in the case of monomial algebras as some derivatives vanish due to the characteristic regardless of what algebra we want to describe. But we can probably work with the divided powers.

The demand that the field is algebraically closed is probably less restrictive, at least if we allow the spectral elements to belong to the algebraic closure of the field. An interesting question related to this is to understand when the spectrum of a subalgebra over the field of complex numbers consists of real elements. It would also be interesting to investigate methods for constructing a SAGBI in this case. The main tool - the existence of a subalgebra B of codimension one less is absent. Though in the real case, we can find a subalgebra of codimension two less.

Perhaps, the most interesting generalization is to allow more than one variable. Here we need to use partial derivatives and for example the monomial subalgebras exhibit a similar description as in the univariate case. Thus there is a realistic hope for the theory to be extendable to several variables. One problem is that it is not clear that the spectrum cannot contain ghost elements if we increase the number of variables.

The main tool—containment in a subalgebra B still works but now we need (in the case of two variables) to speak about (α, β)-derivations. The SAGBI bases seem to be constructed in a similar way and therefore should still be finite. But there are many differences. First of all $f(\alpha, \beta) = 0$ does not give us a factor in $f(x, y)$ which is a fact that we have relied substantially on in the one-dimensional case. Therefore we have no direct analogs for the proofs of theorems corresponding to Theorems 18, 19, 20. It would be interesting to know if they are still valid.

Another difference is that there exists proper subalgebras in $\mathbb{K}[x, y]$ with empty spectrum. An example inspired by [11] is the subalgebra $A = \langle x, xy, xy^2 - y \rangle$.

If we assume that

$$f(\alpha, \beta) = f(\gamma, \delta)$$

for all $f \in A$ and apply this to the generators we find that $\alpha = \gamma, \alpha\beta = \gamma\delta$ and $\alpha\beta^2 - \beta = \gamma\delta^2 - \gamma$. If $\beta \neq \delta$ then $\alpha = \gamma = 0$. Now this in turn implies that $\beta = \delta$. We conclude that $(\alpha, \beta) = (\gamma, \delta)$ so the pair (α, β) was not in the spectrum of A.

Similarly

$$af'_x(\alpha, \beta) + bf'_y(\alpha, \beta) = 0$$

applied to x gives $a = 0$. Thus $b \neq 0$ and application to xy gives $\alpha = 0$. But then

$$b(xy^2 - y)'_y(0, \beta) = -b \neq 0.$$

To check that it is a proper subalgebra suppose that

$$y = F(x, xy, xy^2 - y).$$

If we put $y = \frac{1}{x}$ here then we obtain $\frac{1}{x} = F(x, 1, 0)$ - a contradiction.

In fact no y^k belongs to A and we have, as expected, infinite codimension while $\mathbb{K}[x, y]$ is the only subalgebra of finite codimension that contains A.

But it is impossible to construct similar examples with finite codimension or in the one-variable case.

An interesting question is to find a homological interpretation of our results. Some kind of homological algebra should lie under the surface here.

The characteristic polynomial is especially interesting. What is the most natural way to define it? Can it be introduced for several variables? Can it be interpreted as the characteristic polynomial of some operator on V^2 or $V \times V^*$, where $V = \mathbb{K}[x]/A$?

There are also fundamental open questions regarding the size of the spectrum. Is it an inner property of subalgebra? As $\langle x^2 \rangle$ has an infinite spectrum, the size of the spectrum probably depends on the embedding of the subalgebra in $\mathbb{K}[x]$. But maybe this is not the case if we restrict ourselves by finite codimension only.

There are potential applications to important mathematical problems. We believe that the spectrum will prove to be a useful tool when comparing subalgebras.

We also hope to find some applications in cryptography because we have two essentially different ways to describe subalgebras.

Acknowledgements We are thankful to our mathematical department which gave us the opportunity to work on this project despite the difficult pandemic situation. The starting point of this project was the Bachelor Thesis defence of the first author, where the last author was the scientific advisor and the third was the opponent. It was the observation that the subalgebra $\langle x^3 - x, x^2 \rangle$ can be defined by the condition $f(1) = f(-1)$ that gave the last author the idea to study subalgebra conditions. He conjectured that the main theorem would hold, introduced the main definitions and a plan for how the theorem could be proven. During one year we divided between us different parts of the work to carry out this plan and discussed how to develop the ideas. Trying to classify together the subalgebras of type (3, 4) we got the idea of the characteristic polynomial and the spectrum. The idea to use derivations came much later but became a main tool in the induction approach. SAGBI bases was always the important tool. Prof. Arne Meurman was always participating in our regular meetings and we are very thankful to him for his valuable remarks. Another student, Hugo Eberhard, was participating in part of the discussions as well. We would also like to thank him. Later another student, the second author, joined the project and actively participated in carrying out the classification. Last but not least, we would like to thank our anonymous referees for careful reading and valuable advice that helped improve this article. We were glad to share the joy of being a mathematician and do not consider the project as finished. But somewhere we need to set a point and publish the results obtained so far.

Funding Open access funding provided by Lund University.

References

1. Torstensson, A., Ufnarovski, V., Öfverbeck, H.: On SAGBI bases and resultants. Commutative algebra, singularities and computer algebra (Sinaia, 2002), NATO Sci. Ser. II Math. Phys. Chem., vol. 115, pp. 241–254. Kluwer Academic Publishers, Dordrecht (2003)
2. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra, vol. 2. Springer, Berlin (2005). ISBN: 978-3-540-25527-7; 3-540-25527-3
3. Robbiano, L., Sweedler, M.: Subalgebra Bases, Commutative Algebra (Salvador, 1988), pp. 61–87. Springer, Berlin (1990)
4. Gorin, E.A.: Subalgebras of finite codimension. Math. Notes Acad. Sci. USSR **6**, 649–652 (1969). https://doi.org/10.1007/BF01119685
5. Cox, D.A., Little, J., O'Shea, D.: Using Algebraic Geometry. Graduate Texts in Mathematics. Springer, New York (2005). ISBN: 0-387-20706-6
6. Prasolov, V.V.: Polynomials. Springer, Berlin (2010)
7. Villard, G.: On computing the resultant of generic bivariate polynomials. In: ISSAC'18—Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation, pp. 391–398. New York (2018)
8. Bourbaki, N.: Algebra II: Chapters 4–7. Elements of Mathematics. Springer (1990). English paperback edition
9. Lefler, E.: Derivations in univariate polynomial subalgbras of finite codimension. Bachelor's thesis, Lund Institute of Technology (2021): K39, ISSN 1654-6229, LUFTMA-4007-2021
10. Grönkvist, R., Leffler, E., Torstensson, A., Ufnarovski, V.: Describing subalgebras of $\mathbb{K}[x]$ using derivations (2021). arXiv:2017.11916 [math.RA]
11. Newman, D.J.: Point separating algebras of polynomials. Am. Math. Mon. **81**, 496–498 (1974)