Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 43 (2002), No. 2, 565-577.

Canonical Bases for Subalgebras on Two Generators in the Univariate Polynomial Ring

Anna Torstensson

Centre for Mathematical Sciences, Lund University
Box 118, SE-221 00 Lund, Sweden
e-mail: annat@maths.lth.se

Abstract. In this paper we examine subalgebras on two generators in the univariate polynomial ring. A set, S, of polynomials in a subalgebra of a polynomial ring is called a canonical basis (also referred to as SAGBI basis) for the subalgebra if all lead monomials in the subalgebra are products of lead monomials of polynomials in S. In this paper we prove that a pair of polynomials $\{f, g\}$ is a canonical basis for the subalgebra they generate if and only if both f and g can be written as compositions of polynomials with the same inner polynomial h for some h of degree equal to the greatest common divisor of the degrees of f and g. Especially polynomials of relatively prime degrees constitute a canonical basis. Another special case occurs when the degree of g is a multiple of the degree of f. In this case $\{f, g\}$ is a canonical basis if and only if g is a polynomial in f.

1. Canonical bases for subalgebras

When studying subalgebras of the polynomial ring it is important to construct convenient bases which can be used for example to determine whether a given element is in the subalgebra. Given a finite set of generators for an ideal it is algorithmic to construct a so-called Gröbner basis for the ideal which has this property.

The concept of SAGBI basis, where SAGBI is an abbreviation for Subalgebra Analog to Gröbner Bases for Ideals, was introduced by Kapur and Madlener [5] and independently by Robbiano and Sweedler [9]. They also present a method for constructing such bases given a set of generators for a subalgebra of a multivariate polynomial ring. In general this method is not algorithmic but when dealing with subalgebras of $k[x]$, the polynomial ring in one variable, it can be shown to terminate after a finite number of steps.

Here we will take a closer look at how this construction algorithm works in the case of two generators. The objective is to find a direct criterion for determining if a pair of polynomials is a SAGBI basis.

2. Basic definitions and notation

Let $k[x]$ denote the polynomial ring in one variable with coefficients in the field k. For convenience we will assume that k is of characteristic zero throughout this paper, even though some of the results hold for arbitrary characteristic. The terms in $k[x]$ are the elements x^j, $j \in \mathbb{N}$. A term multiplied by an element of the field is called a monomial. The terms are naturally ordered by the rule $x^j \succ x^k$ if $j > k$. The lead term of a polynomial f is denoted $\mathrm{lt}(f)$ and the lead monomial $\mathrm{lm}(f)$. For a set $S \subseteq k[x]$ we let $\mathrm{lt}(S) = \{\mathrm{lt}(f) | f \in S\}$. The subalgebra A of $k[x]$ generated by S (and containing the field k) is denoted $k[S]$, since it consists of all polynomials in the elements of S. An S-power product is a finite product of elements in S. If P is an S-power product we let $\exp(P)$ denote the corresponding exponent function on S. In other words if $P = \prod_{i=1}^{m}(f_i)^{d_i}$, all f_i different elements of S, then $\exp(P)(f_i) = d_i$ and $\exp(P)$ is zero on all other elements of S.

We can now define our main concept SAGBI basis.

Definition 1. *Let A be a subalgebra of $k[x]$, the polynomial ring in one variable, and $S \subseteq A$. S is a SAGBI basis for A if the lead term of every element in A is an $\mathrm{lt}(S)$-power product.*

Remark. If S is a SAGBI basis for A then A must be the subalgebra generated by S. This can be seen in the following way. It is clear that $k[S] \subseteq A$ since A is a subalgebra. Given an element $a \in A$ we know that the lead term is an $\mathrm{lt}(S)$-power product. After subtraction of the corresponding S-power product, p_1, we get a new element $a - p_1$ in A with lower lead term. Continuing this process we will eventually end up with an element $b = a - p_1 - p_2 - \ldots - p_n$ of $k \subseteq k[S]$ since the degree of the lead term decreases strictly in each subtraction. Hence $a = p_1 + p_2 + \ldots + p_n + b \in k[S]$. This shows that $A = k[S]$. Henceforth we will use the convention to say that S is a SAGBI basis, without specifying a subalgebra, when S is a SAGBI basis for $k[S]$.

Remark. Note that the truth of the condition in the definition of SAGBI basis as well as $k[S]$ is unaffected by multiplying the polynomials in S by non-zero constants. When checking if a set is a SAGBI basis we may therefore assume that all polynomials are monic. Whenever convenient we will use this fact without any further comment. By the same kind of argument we find that we may assume that the constant terms of the polynomials are zero.

What we need now is a procedure for testing if a set is a SAGBI basis. Such a procedure can be found in the paper by Robbiano & Sweedler ([9]). They deal with the more general case of subalgebras of $k[x_1, x_2, \ldots, x_n]$. Even though we will follow their approach closely some smaller simplifications will be possible when working with the univariate case. For a convenient description of the testing procedure we first have to introduce the concept of critical pairs.

Definition 2. *Let A be a subalgebra of $k[x]$. Then a pair (P_1, P_2) of A-power products is a critical pair of A if* $\mathrm{lt}(P_1) = \mathrm{lt}(P_2)$*. If $a \in k$ is such that* $\mathrm{lm}(P_1) = a\ \mathrm{lm}(P_2)$ *we define the T-polynomial of (P_1, P_2) as $T(P_1, P_2) = P_1 - aP_2$.*

Remark. The T-polynomial is constructed in such a way that the lead term of $T(P_1, P_2)$ is smaller than the lead terms of P_1 and P_2.

Definition 3. *If S is the set of critical pairs of A then $T \subseteq S$ is said to generate S if for each (P_1, P_2) in S there exist (Q_i, R_i) with either $(Q_i, R_i) \in T$ or $(R_i, Q_i) \in T$ such that* $\exp(P_1) = \sum_i m_i \exp(Q_i)$ *and* $\exp(P_2) = \sum_i m_i \exp(R_i)$ *for some m_i in k.*

From [9] we have the following theorem.

Theorem 4. *Let S be a subset of $k[x]$ and let T be a set which generates the critical pairs of S. Then S is a SAGBI basis if and only if for each critical pair (P_1, P_2) in T there exist λ_i in k and S-power products Q_i with* $\mathrm{lt}(Q_i) < \mathrm{lt}(P_1) = \mathrm{lt}(P_2)$ *such that*

$$T(P_1, P_2) = \sum_i \lambda_i Q_i. \tag{1}$$

Let us now consider the case of two polynomials f, g in one variable. In this case we can find a particularly simple set of generators for all critical pairs. If $\deg(f) = n$ and $\deg(g) = m$ and $n' = n/(n, m)$, $m' = m/(n, m)$ then it is easy to see that $(f^a g^b, f^c g^d)$ is a critical pair exactly when $(a, b, c, d) = (a, b, a - m'r, b + n'r)$ for some integer r. Thus a set of generators for the critical pairs is given by $\{(f^{m'}, g^{n'})\} \bigcup \{(f^a g^b, f^a g^b) | a, b \in \mathbb{N}\}$ since we can write $(a, b, a - m'r, b + n'r)$ as $(a - rm', b, a - rm', b) + r(m', 0, 0, n')$. Observe that all elements $(f^a g^b, f^a g^b)$ trivially satisfy the condition in Theorem 4 so $\{f, g\}$ is a SAGBI basis if and only if $(f^{m'}, g^{n'})$ satisfies the condition.

We conclude this section with a lemma which shows that the SAGBI basis property is preserved by composition. Here we only prove the simplest case of two polynomials in one variable which suffices for our needs. A more general result can be found in Nordbeck [7].

Lemma 5. *If $\{F, G\} \subseteq k[x]$ is a SAGBI basis and h any polynomial in $k[x]$ then $\{f = F \circ h, g = G \circ h\}$ is also a SAGBI basis.*

Proof. Let the degrees of F and G be n and m, $d = (n, m)$ and $n' = n/d$, $m' = m/d$. According to Theorem 4 and the comment thereafter we can find c_{ij} such that

$$F^{m'} - G^{n'} = \sum c_{ij} F^i G^j$$

where the summation is over (i, j) with $i \deg(F) + j \deg(G) < \deg(F)m' = dn'm'$. After the substitution $x = h(x)$ we get the identity

$$f^{m'} - g^{n'} = \sum c_{ij} f^i g^j$$

Here we see that $i \deg(f) + j \deg(g) < dn'm' \deg(h) = \deg(f)m'$ by multiplying the previous inequality by $deg(h)$. This proves that $\{f, g\}$ is a SAGBI basis by Theorem 4 using the observation

$$\frac{\deg(f)}{(\deg(f), \deg(g))} = \frac{\deg(h)\deg(F)}{\deg(h)(\deg(F), \deg(G))} = n'$$

and similarly for g. $\square$

3. A motivating example

Let us first, in order to understand some of the ideas used later on, look at the case when f is a polynomial of degree two.

Proposition 6. *If $f, g \in k[x]$ with $\deg(f) = 2$ and $\deg(g)$ odd then $\{f, g\}$ is a SAGBI basis.*

Proof. Let $\deg(g) = 2k+1$,

$$f = x^2 + a_1 x + a_0$$
$$g = x^{2k+1} + b_{2k}x^{2k} + \cdots + b_1 x + b_0.$$

We may assume that $a_1 = 0$ since $\{f, g\}$ is a SAGBI-basis if $\{f \circ \Theta^{-1}, g \circ \Theta^{-1}\}$ is, where $\Theta(x) = x + \frac{a_1}{2}$, by Lemma 5.

According to the definition $\{f, g\}$ is a SAGBI-basis if the lead term of any polynomial in f and g is a product of lead terms of f and g, that is either is of degree greater than $2k$ or of even degree. Assume that $\{f, g\}$ is not a SAGBI basis. Then there must be a polynomial $p(x, y)$ such that $p(f(x), g(x))$ is of odd degree less than $2k$. Since any polynomial in $\{f, g\}$ is a polynomial in $\{x^2, g\}$ it follows that $\{x^2, g\}$ is no SAGBI basis. Thus, it suffices to show that $\{x^2, g\}$ is a SAGBI basis.

Using the algorithm for verification of SAGBI bases given in the previous section we only have to check that $g^2 - x^{4k+2}$ can be written as a polynomial in g and x^2 where the degree of each term, regarded as polynomial in x, is less than $4k+2$. Let g_0 and g_1 be the even and odd parts of g respectively. Note that g_0 is a polynomial in x^2. Then we can write

$$g^2 - x^{4k+2} = g_0^2 + 2g_0 g_1 + g_1^2 - x^{4k+2} = 2g_0 g - g_0^2 + g_1^2 - x^{4k+2}$$

which gives our desired representation since g_1^2 is even and the lead monomials of g_1^2 and x^{4k+2} cancel so that the degree requirement is fulfilled. $\square$

When g is of even degree the situation is slightly more complicated.

Proposition 7. *If $f, g \in k[x]$ with $f = x^2 + a_1 x + a_0$ and $\deg(g)$ even then $\{f, g\}$ is a SAGBI-basis if and only if $h(x) = g(x - \frac{a_1}{2})$ is an even polynomial.*

Remark. The condition that $h(x)$ is even is equivalent to g being a polynomial in f: If

$$g(x) = \sum_{i=0}^{s} \alpha_i f(x)^i = \sum_{i=0}^{s} \alpha_i ((x + \frac{a_1}{2})^2 - \frac{a_1^2}{4} + a_0)^i$$

then

$$h(x) = g(x - \frac{a_1}{2}) = \sum_{i=0}^{s} \alpha_i (x^2 - \frac{a_1^2}{4} + a_0)^i$$

which is clearly even. If, on the other hand,

$$g(x - \frac{a_1}{2}) = \sum_{i=0}^{s} \alpha_{2i} x^{2i}$$

then we can find β_i such that

$$g(x - \frac{a_1}{2}) = \sum_{i=0}^{s} \beta_{2i}(x^2 - \frac{a_1^2}{4} + a_0)^i$$

in other words

$$g(y) = \sum_{i=0}^{s} \beta_{2i} f(y)^i$$

so g is a polynomial in f.

Proof. Let $\deg(g) = 2k$,

$$f(x) = x^2 + a_1 x + a_0,$$
$$g(x) = x^{2k} + b_{2k-1}x^{2k-1} + \cdots + b_1 x + b_0,$$

and again let $\Theta(x) = x + \frac{a_1}{2}$. Using our Lemma 5 for composition with both Θ and Θ^{-1} we conclude that $\{f, g\}$ is a SAGBI basis if and only if $\{f \circ \Theta^{-1}, g \circ \Theta^{-1}\}$ is.

In this case the SAGBI basis verification consists of checking if $g \circ \Theta^{-1} - (f \circ \Theta^{-1})^k$ or equivalently $h = g \circ \Theta^{-1}$ is an even polynomial. □

In the next section we will generalize the first case here to the statement that any pair of polynomials in $k[x]$ with degrees that are relatively prime constitute a SAGBI basis.

4. Polynomials of relatively prime degrees

In the proof of Proposition 6 we used the fact that we could (uniquely) write $g = g_0 + g_1$ where g_0 is an even and g_1 an odd polynomial. For the general case we use a generalization of this fact stated in the proposition below. The proof is a standard argument in commutative algebra, but we include it for the sake of completeness.

Proposition 8. *Let f be a polynomial of degree n. Then*

$$k[x] = k[f] \oplus xk[f] \oplus x^2 k[f] \oplus \cdots \oplus x^{n-1}k[f].$$

Proof. We first note that $\{1, x, x^2, \ldots, x^{n-1}\}$ generates $k[x]$ as $k[f]$ module since x satisfies the degree n polynomial $F(f, y) = f(y) - f \in k[f][y]$. To show that $\{1, x, x^2, \ldots, x^{n-1}\}$ is a set of free generators we observe that if we have

$$q_0(f) + q_1(f)x + \cdots + q_k(f)x^k = 0,$$

by reducing the exponents of the lead terms in each $q_i(f)x^i$ modulo n we find that they are all incongruent. Hence there can be no cancellation of lead terms on the LHS and it follows that all q_i must be zero. We conclude that $\{1, x, x^2, \ldots, x^{n-1}\}$ is a free generating set. □

The following lemma gives a convenient alternative to the condition on the non-trivial T-polynomial given in the SAGBI test theorem.

Lemma 9. *Let $f, g \in k[x]$ be of relatively prime degrees n and m respectively. If there are polynomials p_i such that*

$$g^n = p_{n-1}(f)g^{n-1} + p_{n-2}(f)g^{n-2} + \cdots + p_1(f)g + p_0(f) \tag{2}$$

then $\{f, g\}$ is a SAGBI basis.

Proof. By Theorem 4 it suffices to show that the T-polynomial $T(f, g) = g^n - f^m$ has a representation of the form (1). We will see that the above equality will give us such a representation after finding a term f^m on the RHS and moving it to the LHS. We first note that the greatest exponents of x in the different terms on the RHS all are incongruent modulo n. The lead term in g^n is x^{mn}. Due to the incongruency, the only place on the RHS where we can find such a term is $p_0(f)$. It follows that p_0 is of degree m so $p_0(f)$ contains the term f^m that we are looking for. It only remains to check that the degree requirement in (1) is satisfied, that is that all $\{f, g\}$-power products on the RHS are of degree less than mn. It is enough to check the lead terms in each $p_i(f)g^i$. After removal of f^m from $p_0(f)$ the lead term is of degree at most $(m-1)n$. Since all the lead terms left on the RHS have incongruent exponents they cannot cancel each other. On the other hand the lead term on the LHS after subtracting f^m is of degree less than mn. Hence the terms on the RHS must also be of degree less than mn so we have a representation of $T(f, g)$ of the desired form. □

We have now gathered all the tools we need to prove the main theorem of this section.

Theorem 10. *If $f, g \in k[x]$ are of degrees that are relatively prime then $\{f, g\}$ is a SAGBI basis.*

Proof. Let n and m be the degrees of f and g respectively. According to Lemma 9 it is enough to prove the existence of polynomials $p_0, p_1, \ldots, p_{n-1}$ such that

$$g^n = p_{n-1}(f)g^{n-1} + p_{n-2}(f)g^{n-2} + \cdots + p_1(f)g + p_0(f) \tag{3}$$

We know from Proposition 8 that $k[x]$ is a finitely generated $k[f]$-module that has a generating set of cardinality n. By Proposition 2.4 in [2] g is integral over $k[f]$ and from the proof given there it is clear that the degree of the equation g satisfies equals the number of generators of $k[x]$. In other words equation (3) holds. □

One natural question to ask given a set of generators is whether they generate the whole of $k[x]$ or not. In terms of SAGBI bases this is the question whether a SAGBI basis contains an element of degree one or not. The above theorem immediately gives us a partial answer to this question in the case of two generators.

Corollary 11. *If f, g in $k[x]$ are of degrees at least two that are relatively prime then $k[f, g] \neq k[x]$.*

Proof. By Theorem 10 $\{f, g\}$ is a SAGBI basis of $k[f, g]$. Hence all elements in $k[f, g]$ have a lead term that is a product of $\mathrm{lt}(f)$ and $\mathrm{lt}(g)$ so x cannot be in the subalgebra. □

A generalization of this can be found in [1] (Theorem 9.11, p. 71). Here it is proven that if $k[f, g] = k[x]$ then we must have either $\deg(f) | \deg(g)$ or $\deg(g) | \deg(f)$. An example of such polynomials is $k[x^n, x^{nk} + x] = k[x]$. The condition of one degree dividing the other is not sufficient for generating $k[x]$ as the example $k[x^n, x^{nk}] = k[x^n] \neq k[x]$ shows.

5. A general criterion

In this section we will prove a general criterion for pairs of polynomials to form a SAGBI basis, but first we examine another special case. The general criterion is a natural generalization of the discoveries we will make about this special case.

In the previous section we considered pairs of polynomials such that the degrees had no common factor. We will now turn to the case at the other extreme, when one degree divides the other.

Theorem 12. *Let $f, g \in k[x]$ be such that $\deg(f) | \deg(g)$. Then $\{f, g\}$ is a SAGBI-basis if and only if g is a polynomial in f.*

Proof. Let $\deg(f) = n$ and $\deg(g) = m = nk$. We once again use the unique representation of g as $g = g_0(f) + xg_1(f) + x^2g_2(f) + \cdots + x^{n-1}g_{n-1}(f)$ from Lemma 8. By Theorem 4 a criterion for being a SAGBI-basis is that the T-polynomial

$$g - f^k = (g_0(f) - f^k) + xg_1(f) + x^2g_2(f) + \cdots + x^{n-1}g_{n-1}(f)$$

has a representation of the form (1), in this case that it is a polynomial in f of degree less than k. By the uniqueness part of Lemma 8 this is possible exactly when g is a polynomial in f. $\square$

Let $d = (\deg(f), \deg(g))$. Note that in both cases treated above, $d = 1$ and $d = \deg(f)$, the condition for being a SAGBI basis is that there is a polynomial h of degree d such that both f and g can be written as polynomials in h. (When $d = 1$ this condition is trivially satisfied since we may choose h as x.) Our main theorem is that this generalizes to arbitrary degrees. To prove that a given SAGBI basis has this form we will use a result from [6] (Lemma 1.33, p.136) saying that for any field between k and $k(x)$ that contains some polynomial of positive degree, one can find a polynomial that generates this intermediate field. We will combine that result with the following:

Lemma 13. *For any polynomial $h \in k[x]$ we have $k[h] = k(h) \cap k[x]$.*

Proof. The inclusion $k[h] \subseteq k(h) \cap k[x]$ is clear. Let $f \in k(h) \cap k[x]$ so there are polynomials a and b such that $f = \frac{a \circ h}{b \circ h}$. Note that $\deg(f) = \deg(a)\deg(h) - \deg(b)\deg(h)$ and hence $\deg(h)|\deg(f)$. We will show that $f \in k[h]$ by induction on the degree of f. Assume that $\deg(f) < \deg(h)$. Then $\deg(f) = 0$ so the statement $f \in k[h]$ holds in this case. For f of higher degree there is a γ with $\deg(f) = \gamma \deg(h)$. Then we can find a $c \in k$ such that $\widetilde{f} = f - ch^\gamma$ has lower degree than f. By the induction hypothesis it follows that $\widetilde{f} = \frac{a \circ h}{b \circ h} - ch^\gamma$ is in $k[h]$ and hence f is. $\square$

Remark. Note that the above lemma cannot be generalized to several generators. For instance $k[x^2, x^3] \neq k(x^2, x^3) \cap k[x]$ since $x = \frac{x^3}{x^2} \in k(x^2, x^3) \cap k[x]$ but $x \notin k[x^2, x^3]$ by Corollary 11.

Theorem 14. *Let $f, g \in k[x]$ and $d = (\deg(f), \deg(g))$. Then $\{f, g\}$ is a SAGBI basis if and only if there is a polynomial $h \in k[x]$ of degree d and polynomials F, G such that $f = F \circ h$ and $g = G \circ h$.*

Proof. The sufficiency follows from our earlier results: The degree of F and G are relatively prime so they form a SAGBI basis by Theorem 10. Now we only have to invoke Lemma 5 to see that $\{f, g\}$ is a SAGBI basis.

The proof of the necessity relies on a result from [6] that any field between k and $k(x)$ containing a nonconstant polynomial has a single generator lying in $k[x]$. Applying this result to $k(f, g)$ we find a polynomial h such that $f, g \in k[x] \cap k(h)$ so $f, g \in k[h]$ by Lemma 13. Hence there are polynomials F and G such that $f = F \circ h$ and $g = G \circ h$. It only remains to show that h is of degree d. It is obvious that $\deg(h) | \deg(f), \deg(g)$ and hence $\deg(h)|d$. On the other hand $h = P(f,g)/Q(f,g)$ for some polynomials P and Q. Now the fact that $\{f, g\}$ is a SAGBI basis ensures that the lead terms of $P(f, g)$ and $Q(f, g)$ are $\{\mathrm{lt}(f), \mathrm{lt}(g)\}$-power products. But then their degrees in x must be linear combinations of $\deg(f)$ and $\deg(g)$ and hence divisible by d. It follows that $d| \deg(P(f, g)) - \deg(Q(f, g)) = \deg(h)$. We have seen above that $\deg(h)|d$ so clearly we can draw our desired conclusion $\deg(h) = d$. □

Note that the proof for the necessity holds for an arbitrary (finite) number of polynomials. The sufficiency, on the contrary, does not hold even for three polynomials as the following example shows.

Example. The set $\{x^2 - x, x^3, x^5\}$ is not a SAGBI basis even though the degrees of the polynomials have no common factor. (Note that the degrees are even pairwise relatively prime in this example.) For instance $x^5 - (x^2 - x)x^3 - (x^2 - x)^2 - 2x^3 + (x^2 - x) = -x$ is a polynomial in $x^2 - x$, x^3 and x^5 with lead term $-x$ which obviously cannot be written as a product of the lead terms of the generators.

Next we will see that a simple representation of the T-polynomial of $\{f, g\}$ is related to F and G being polynomials of a simple type.

Theorem 15. *If the only non-trivial T-polynomial of $\{f, g\}$ is zero then f and g are both powers of a polynomial of degree* $(\deg(f), \deg(g))$.

Proof. Let $n = \deg(f)$, $m = \deg(g)$, $d = (n, m)$, $n' = n/d$ and $m' = m/d$. Then the condition in the theorem is that $f^{m'} = g^{n'}$. Let $f = \prod_{i=1}^{n}(x - \alpha_i)$ and $g = \prod_{j=1}^{m}(x - \beta_j)$. Then any root γ of f of multiplicity j is a root of multiplicity $m'j$ of $f^{m'} = g^{n'}$. Now any root of $g^{n'}$ must have multiplicity $n'k$ for some k. It follows from $m'j = n'k$ that $m'|k$ and $n'|j$ so γ has multiplicity a multiple of $n'm'$. Since this holds for any root $f^{m'} = g^{n'} = \prod_{i=1}^{t}(x - \gamma_i)^{m'n'j_i}$ so we find that both f and g are powers of $\prod_{i=1}^{t}(x - \gamma_i)^{j_i}$. □

If we want to check if a given pair of polynomials is a SAGBI basis the following characterization of when a polynomial can be written as a composition may be useful.

Proposition 16. *Let h be a polynomial of degree d and f a polynomial of degree $n = dn'$ with zeroes $\alpha_1, \alpha_2, \dots, \alpha_n$. Then f is of the form $F \circ h$ for some polynomial F if and only if there are $\beta_1, \beta_2, \dots, \beta_{n'}$ such that the zeroes of f can be partitioned into n' multisets M_i where M_i contains the zeroes of $h(x) - \beta_i$.*

Proof. Assume that $f = F \circ h$ where $F(x) = \prod_{i=1}^{n'}(x - \beta_i)$. Then $f(x) = \prod_{i=1}^{n'}(h(x) - \beta_i)$ so $h(\alpha_i) = \beta_j$ for some j that is α_i is a zero of $h(x) - \beta_j$. Divide out this factor and continue in the same way. It follows that $[h(\alpha_1), h(\alpha_2), \ldots, h(\alpha_n)]$ and $[(\beta_1, d), (\beta_2, d), \ldots (\beta_{n'}, d)]$ are equal as multisets.

For the other direction we assume that there are β_i's such that $h(x) - \beta_i$ has d zeroes among the α_i's. Then $\prod_{i=1}^{n'}(h(x) - \beta_i) = \prod_{i=1}^{n}(x - \alpha_i) = f(x)$ and hence $f = F \circ h$ where $F = \prod_{i=1}^{n'}(x - \beta_i)$. □

Remark. This gives us another criterion for $\{f, g\}$ of degrees 2 and $2k$ to be a SAGBI basis. We know that it is equivalent to g being a polynomial in f. According to the above proposition the latter is equivalent to the possibility to partition the zeroes of g into pairs $(\beta_{2j-1}, \beta_{2j})$ such that $f(x) - \gamma_j = (x - \beta_{2j-1})(x - \beta_{2j})$ for some γ_j. That is to say that $\beta_{2j-1} + \beta_{2j} = \alpha_1 + \alpha_2$ where α_1 and α_2 are the zeroes of f.

For polynomials where the gcd of the degrees is 2 some calculations for polynomials of low degrees suggested a different description of all pairs of polynomials that are SAGBI bases. Next we will describe this alternative condition and show that it is equivalent to the condition given in Theorem 14 above.

Theorem 17. *If both f and g are of even degree then both of them are polynomials in some polynomial of degree 2 if and only if there is a constant s such that*

$$f = f_0 - \sum_{k=1}^{\infty} \frac{\alpha_{k+1} s^k f_0^{(k)}(x)}{(k+1)!}$$

and

$$g = g_0 - \sum_{k=1}^{\infty} \frac{\alpha_{k+1} s^k g_0^{(k)}(x)}{(k+1)!}$$

where f_0 and g_0 are the even parts of f and g respectively and α_k the Genocchi numbers.

Remark. The Genocchi numbers can be defined by $\alpha_k = 2(1 - 2^k)B_k$ where B_k are the more well known Bernoulli numbers or by their exponential generating function $\frac{2x}{1+e^x}$ (See for example [4].)

Proof. From the definition $\frac{2x}{1+e^x} = \sum_{k=1}^{\infty} \frac{\alpha_k x^k}{k!}$ using that $\alpha_1 = 1$ it follows that $\left(\frac{1+e^{-x}}{2}\right)\left(1 - \sum_{k=1}^{\infty} \frac{\alpha_{k+1} x^k}{(k+1)!}\right) = 1$. If we substitute x by sD that is multiplication by s and differentiation with respect to x we get an identity between operators where the second factor applied to f_0 is the RHS of the condition on f stated in the theorem. Hence the condition is equivalent to the existence of an s such that $\left(\frac{1+e^{-sD}}{2}\right)(f) = f_0$. (Here 1 denotes the identity operator.) The left hand side evaluated in x is just $\frac{f(x)+f(x-s)}{2}$ so the condition in the theorem can be formulated as follows. There exists an s such that $\frac{f(x)+f(x-s)}{2} = \frac{f(x)+f(-x)}{2}$ and $\frac{g(x)+g(x-s)}{2} = \frac{g(x)+g(-x)}{2}$. By factorization of the identity $f(-x) = f(x - s)$ it is easy to realize that this is equivalent to the possibility to partition the zeroes of f into pairs with sum $-s$. This concludes the proof by the remark after Proposition 16. □

We will make some general remarks on the nature of the condition in the above theorem but let us first examine an example.

Example. We will describe all SAGBI bases $\{f, g\}$ where f and g are of degrees 4 and 6 respectively. Combining the above theorem with Theorem 14 we know that $\{f, g\}$ is a SAGBI basis if and only if

$$f = f_0 - \sum_{k=1}^{4} \frac{\alpha_{k+1} s^k f_0^{(k)}(x)}{(k+1)!} = f_0 + \frac{sf_0'}{2} - \frac{s^3 f_0^{(3)}}{24}$$

and

$$g = g_0 - \sum_{k=1}^{6} \frac{\alpha_{k+1} s^k g_0^{(k)}(x)}{(k+1)!} = g_0 + \frac{sg_0'}{2} - \frac{s^3 g_0^{(3)}}{24} + \frac{s^5 g_0^{(5)}}{240}$$

Letting $f = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ and $g = x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ the conditions are

$$f = x^4 + 2sx^3 + a_2x^2 + (a_2s - s^3)x + a_0$$

and

$$g = x^6 + 3sx^5 + b_4x^4 + (2sb_4 - 5s^3)x^3 + b_2x^2 + (sb_2 - s^3b_4 + 3s^5)x + b_0$$

or equivalently there exists an s such that $a_3 = 2s, a_1 = a_2s - s^3, b_5 = 3s, b_3 = 2sb_4 - 5s^3, b_1 = sb_2 - s^3b_4 + 3s^5$. As we can see the coefficients of the even terms in f and g and s can be chosen freely but then all coefficients of the odd terms are uniquely determined. Thus all SAGBI basis $\{f, g\}$ with monic polynomials of degrees 4 and 6 can be parameterized by 6 parameters. If we do not require the polynomials to be monic we get 8 parameters since we may multiply f and g by arbitrary constants. This example suggests that the above theorem gives a convenient criterion both for generating SAGBI bases with two elements of given (appropriate) degrees and for checking if two given polynomials constitute a SAGBI basis.

Corollary 18. *All SAGBI bases $\{f, g\}$ where $\deg(f) = 2u$ and $\deg(g) = 2v$, $(u, v) = 1$ can be parameterized by $u + v + 3$ parameters.*

Proof. By Theorem 14 the condition in Theorem 17 gives a SAGBI basis criterion when $\deg(f) = 2u$, $\deg(g) = 2v$ and $(u, v) = 1$. We just have to show that the conditions on f and g are such that s and all coefficients of even terms (there are $u + v + 2$ such terms) can be chosen freely but all odd coefficients are uniquely determined after these choices have been made. Let us therefore take a closer look at the condition on f:

$$f = f_0 - \sum_{k=1}^{2u+1} \frac{\alpha_{k+1} s^k f_0^{(k)}(x)}{(k+1)!} \tag{4}$$

It is easy to see that all α_k for odd $k \geq 3$ are zero. (Just check that the generating function of α_k becomes even after removal of $\alpha_0 + \alpha_1 x = x$ or equivalently that $\frac{2x}{1+e^x} - x$ is even.) This means that we only have to sum over odd k in (4). But then all derivatives of f_0 in the sum are of odd order and hence give odd polynomials. It follows that all coefficients of even powers of x are equal on both sides for any f. Let us compare coefficients of odd powers of

x. Let $f = \sum_{i=0}^{2u} a_i x^i$ and t be an odd number between 1 and $2u-1$. The coefficient of x^t on the LHS is a_t. The RHS equals

$$f_0 - \sum_{k=1}^{2u+1} \frac{\alpha_{k+1} s^k}{(k+1)!} \sum_{l=\frac{k+1}{2}}^{u} a_{2l} \frac{(2l)!}{(2l-k)!} x^{2l-k}$$

so the coefficient of x^t equals

$$-\sum_{k=1}^{2u-t} \frac{\alpha_{k+1} s^k}{k+1} \binom{t+k}{t} a_{t+k}$$

Equating the coefficients on both sides we get an expression for a_t in s and a_r for even $r > t$. We may of course reformulate the condition on g in the same way so this proves that we may choose all $u+v+2$ coefficients of even powers and the parameter s arbitrarily and that this determines f and g. □

Corollary 19. *The monic polynomials of degree $2k$ that can be written as $F \circ h$ for some h of degree 2 are those of the form*

$$f_0 - \sum_{k=1}^{\infty} \frac{\alpha_{k+1} s^k f_0^{(k)}(x)}{(k+1)!}$$

where f_0 is any even polynomial of degree $2k$, s the coefficient of x in h and α_k the Genocchi numbers.

Proof. This follows from Theorem 17 by letting g be of degree 2 since the condition on g stated in the theorem is that the coefficient of x equals s. □

6. A remark on the non-commutative case

SAGBI bases can also be defined for subalgebras of the non-commutative polynomial ring in a similar fashion. In that setting we have to redefine concepts like critical pairs and T-polynomials in a suitable way. This is done in Nordbeck [8]. In connection with our discussion it is interesting to mention the following result on subalgebras with two generators in the non-commutative polynomial ring which is mentioned in [3].

Theorem 20. *Let A be a subalgebra of $k\langle X\rangle$, the non-commutative polynomial ring in n variables, generated by two elements f and g. Then either A is a free subalgebra or A is contained in a subalgebra generated by one element.*

Proof. If the generators commute then they are both contained in the centralizer of f which is a one generator subalgebra by Bergman's centralizer theorem. (Theorem 6.7.7 in [3].) Otherwise A is free on f and g by corollory 6.7.4 in [3]. □

In the language of SAGBI bases this can be interpreted in the following way. If there exist no critical pairs then $\{f, g\}$ is a SAGBI basis. Also A is free on the generators $\{f, g\}$ for if we have a relation that f and g satisfies $r(f, g) = 0$ then we must have at least two equal lead monomials on the LHS that cancel. Hence we have found a critical pair contradictory to our assumption. On the other hand if we have a critical pair that can be represented in a way corresponding to (1) then this gives us a relation. This shows that for a subalgebra generated by a two element SAGBI basis freeness is equivalent to the non-existence of product relations between the lead terms of the generators.

The above theorem combined with our earlier results gives a description of two element SAGBI bases in $k\langle X\rangle$:

Theorem 21. *The set $\{f, g\} \subseteq k\langle X\rangle$ is a SAGBI basis if and only if:*

- *There are no critical pairs for $\{f, g\}$.*
- *There is $h \in k\langle X\rangle$ and a SAGBI basis $\{F, G\} \subseteq k[x]$ with $f = F \circ h$ and $g = G \circ h$.*

Proof. Assume that $\{f, g\}$ is a SAGBI basis. By the discussion above either there are no product relations between the lead words or the subalgebra $\langle f, g\rangle$ is contained in a subalgebra $\langle h\rangle$ generated by one element. In the latter case we can write $f = F \circ h$, $g = G \circ h$ for some polynomials F, G. If there is a T-polynomial $T(F, G)$ then we get a representation of type (1) of it by replacing h by x in the representation of $T(f, g) = T(F \circ h, G \circ h)$ and hence $\{F, G\}$ is a SAGBI basis.

Conversely if $\{F, G\} \subseteq k[x]$ is a SAGBI basis then it follows from Nordbeck [7] that $\{f = F \circ h, g = G \circ h\}$ is a SAGBI basis. □

Acknowledgements. I am grateful to my supervisor Victor Ufnarovski for many interesting suggestions and comments. In particular the necessity part of the proof of Theorem 14 and the formulation of Theorem 17 is entirely due to him. I would also like to thank Jörgen Backelin for his suggestions that lead to a simplification of the proof of Theorem 10. Finally thanks to Patrik Nordbeck and Jonas Månsson for interesting discussions and especially for pointing out the relevance of the results presented here for the non-commutative setting. The contents of Section 6 is based on their ideas.

References

[1] Abhyankar, S. S: *Lectures on expansion techniques in algebraic geometry.* Tata Institute of Fundamental Research, Bombay, 1977. Notes by Balwant Singh. Zbl 0818.14001

[2] Atiyah, M. F.; Macdonald, I. G.: *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. Zbl 0175.03601

[3] Cohn, P. M.: *Free rings and their relations.* Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, second edition, 1985. Zbl 0659.16001

[4] Horadam, A. F.: Genocchi polynomials. In: Applications of Fibonacci numbers, Vol. 4 (Winston-Salem, NC, 1990), Kluwer Acad. Publ., Dordrecht 1991, 145–166. Zbl 0749.11019

[5] Kapur, Deepak; Madlener, Klaus: *A completion procedure for computing a canonical basis for a k-subalgebra.* In: Computers and mathematics (Cambridge, MA, 1989), Springer, New York 1989, 1–11. Zbl 0692.13001

[6] Lausch, Hans; Nöbauer, Wilfried: *Algebra of polynomials.* North-Holland Publishing Co., Amsterdam, 1973. North-Holland Mathematical Library, Vol. 5. Zbl 0283.12101

[7] Nordbeck, Patrik: *Sagbi bases under composition.* J. Symbolic Comput., to appear.

[8] Nordbeck, Patrik: *Canonical subalgebra bases in non-commutative polynomial rings.* In: Proc. ISSAC '98 ACM Press 1998, 140–146. Zbl 0927.16045

[9] Robbiano, Lorenzo; Sweedler, Moss: *Subalgebra bases.* In: Commutative algebra (Salvador, 1988). Springer, Berlin 1990, 61–87. Zbl 0725.13013

Received April 9, 2001