

IDEAL AND SUBALGEBRA COEFFICIENTS

LORENZO ROBBIANO AND MOSS SWEEDLER

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. For an ideal or K -subalgebra E of $K[X_1, \dots, X_n]$, consider subfields $k \subset K$, where E is generated – as ideal or K -subalgebra – by polynomials in $k[X_1, \dots, X_n]$. It is a standard result for ideals that there is a smallest such k . We give an algorithm to find it. We also prove that there is a smallest such k for K -subalgebras. The ideal results use *reduced* Gröbner bases. For the subalgebra results we develop and then use *subduced* SAGBI (bases), the analog to *reduced* Gröbner bases.

1. INTRODUCTION

This paper is about subfields $k \subset K$ where $k[X_1, \dots, X_n]$ contains generators for an ideal or K -subalgebra of a polynomial ring $K[X_1, \dots, X_n]$. In the case of an ideal, it is well known that there is a smallest such subfield k . Utilizing *reduced* Gröbner bases, we provide an algorithm which, starting from a finite set of generators for the ideal, produces a finite set of generators for k as a field extension of the prime field.

Suppose that B is a K -subalgebra of the polynomial ring. B may be finitely generated or not. Is there a smallest subfield $k \subset K$ where B is generated by polynomials lying in $k[X_1, \dots, X_n]$? Utilizing SAGBI¹ – and developing the subalgebra analog to *reduced* Gröbner bases – we prove there is. Although we present an algorithm which produces a generating set for the field of definition of an ideal, for a K -subalgebra – even a finitely generated K -subalgebra – we are not able to provide such an algorithm, in general. However, we do prove that for a finitely generated K -subalgebra, the field of definition is finitely generated over the prime field.

2. IDEAL COEFFICIENTS

In the following we use “ $k[X]$ ” to stand for “ $k[X_1, \dots, X_n]$ ”. Here is how the theory of Gröbner bases can be used to prove the following well-known fact.

Received by the editors August 29, 1996 and, in revised form, January 16, 1997.

1991 *Mathematics Subject Classification*. Primary 13P10; Secondary 12Y05.

Key words and phrases. Ideal, subalgebra, field of definition, reduced Gröbner basis, subduced SAGBI (basis).

The first author was partially supported by the Consiglio Nazionale delle Ricerche (CNR).

The second author was partially supported by the United States Army Research Office through the Army Center of Excellence for Symbolic Methods in Algorithmic Mathematics (ACSyAM), Mathematical Sciences Institute of Cornell University, Contract DAAL03-91-C-0027, and by the NSA.

¹The “dictionary” from *Idealish* to *Subalgibberish* translates “ideal” to “subalgebra” and “Gröbner basis” to “SAGBI”. The “reduction” process translates to “subduction”.

Proposition 2.1. *Let $k \subseteq K$ be a field extension and let I be an ideal of $k[X]$. Then*

$$IK[X] \cap k[X] = I.$$

Proof. Choose a term-order σ and let G_σ be a reduced Gröbner basis of I with respect to σ . It is a standard result (see for instance [AL], [E]) that G_σ is uniquely determined by σ , no matter which set of generators of I the Gröbner basis is computed from. Moreover the coefficients of the polynomials in G_σ are obtained by field operations (addition, subtraction, multiplication and division) on the coefficients of the given set of generators. Therefore G_σ is also the reduced Gröbner basis of $IK[X]$. Since $G_\sigma \subset k[X]$, if $f(X) \in k[X]$ then reducing $f(X)$ over G_σ involves repeated *subtracting off* elements of G_σ times polynomials in $k[X]$. Thus if f' is the normal form of f , $f - f' \in k[X]G = I$. If $f(X) \in IK[X] \cap k[X]$, then $f' = 0$ and $f \in I$. \square

Here is the formal definition of an ideal being *defined over* a subfield of K .

Definition 2.2. Let K be a field with subfield L and let I be an ideal in $K[X]$. I is *defined over* L if I is generated as an ideal in $K[X]$ by polynomials lying in $L[X]$. There is a subfield of K over which I is defined and which lies in all other subfields of K over which I is defined, for example see [L58]. This smallest subfield of K over which I is defined is the *field of definition* of I .

Example 2.3. Let $I \subseteq \mathbb{C}[X, Y, Z]$ be the ideal defined by

$$I := (X^2 - \sqrt{5}XY + 3XZ + 2\sqrt{5}Z^2, XY - \sqrt{2}Z^2, 2XY + \sqrt{3}Z^2).$$

It is easy to check that

$$I = (X^2 + 3XZ, XY, Z^2),$$

hence the field of definition of I is \mathbb{Q} .

Theorem 2.4. *Let I be an ideal in $K[X]$, let σ be a term-order, let G_σ be the reduced Gröbner basis of I with respect to σ and let k be the subfield of K generated over the prime field by the coefficients of the polynomials in G_σ . Then k is the field of definition of I .*

Proof. I is defined over k because $G_\sigma \subseteq k[X]$ and I is generated by G_σ as an ideal in $K[X]$.

Now for the “smallestness” of k . Suppose that L is a subfield of K over which I is defined. In fact, suppose that I is generated as an ideal in $K[X]$ by $F_1, \dots, F_r \in L[X]$. Compute G_σ starting from the set of generators $\{F_1, \dots, F_r\}$ for I . Again, the coefficients of the polynomials in G_σ are obtained by field operations (addition, subtraction, multiplication and division) on the coefficients of F_1, \dots, F_r . Hence, the coefficients of the polynomials in G_σ lie in L , and so $k \subseteq L$. \square

Since G_σ is a finite set of polynomials, the set of coefficients of the polynomials in G_σ is a finite generating set over the prime field for the field of definition of I .

Corollary 2.5. *Let $I \subseteq K[X]$ be an ideal for which one has an explicit set of generators. Then the field of definition of I is computable.*

Proof. Let k be the field generated over the prime field by the coefficients of the given set of generators. k is a finitely generated extension of the prime field, hence computable. Thus the conclusion follows from Theorem 2.4. \square

Corollary 2.6. *Let $I \subseteq K[X]$. The subfield of K generated over the prime field by the coefficients of a reduced Gröbner basis of I is independent of the term-order.*

Proof. All these subfields coincide with the field of definition of I . □

Remark 2.7. Let I be an ideal in $K[X]$, σ a term order and $\Omega : K[X] \rightarrow K[X]$ a K -algebra homomorphism. It is not true that I being stable with respect to Ω —meaning $\Omega(I) = I$ —implies that the polynomials of the reduced Gröbner basis of I are Ω -invariant. For instance, let Ξ be the automorphism of $K[X, Y]$ interchanging X and Y . The ideal generated by $X + Y$ and XY is Ξ -stable. $\{X + Y, Y^2\}$ is the reduced Gröbner basis of I with respect to every term order σ such that $X >_{\sigma} Y$. But $\{X + Y, Y^2\}$ is not Ξ -invariant.

The problem is that Ξ does not respect the term order. One way to obtain ring endomorphisms of $K[X]$ which do respect the term order is to begin with a homomorphism $\alpha : K \rightarrow K$. Let $\alpha[X]$ denote the extension of α to $K[X]$ where $\alpha[X]$ applied to a polynomial is simply α applied to the coefficients of the polynomial.² Since $\alpha[X]$ just acts on coefficients, it respects the term order in the sense that for a polynomial f the lead term of $\alpha[X](f)$ is $\alpha[X]$ of the lead term of f . Ξ does not respect the term order in this sense. The lead term of $\Xi(X + Y)$ is not Ξ of the lead term of $X + Y$.

The next result is due to Traverso (see [T]).

Proposition 2.8. *a) Let $\alpha : K \rightarrow K$ be a homomorphism, let $k_{\alpha} \subset K$ be the fixed subfield of α and let $\alpha[X]$ be the extension of α to $K[X]$ defined above. If $\alpha[X]$ carries the ideal I into itself, then the reduced Gröbner basis of I lies in $k_{\alpha}[X]$.*

b) Let K be a Galois extension of k with Galois group $\text{Gal}_k(K)$, and suppose that I is an ideal of $K[X]$ which is stable with respect to $\text{Gal}_k(K)[X]$, where $\text{Gal}_k(K)[X]$ is the group of automorphisms of $K[X]$ consisting of $\alpha[X]$'s for $\alpha \in \text{Gal}_k(K)$. Then the reduced Gröbner basis of I lies in $k[X]$.

Proof. Let σ be a term-order and let G_{σ} be the reduced Gröbner basis of I with respect to σ . Since $\alpha[X]$ respects term orders, it carries a (reduced) Gröbner basis for an ideal J into a (reduced) Gröbner basis for $\alpha[X](J)$. Since I is stable, $\alpha[X]$ carries a reduced Gröbner basis for I to itself. Again, since $\alpha[X]$ acts on the coefficients, and the elements of the reduced Gröbner basis have distinct leading exponents, it follows that $\alpha[X]$ acts trivially on the reduced Gröbner basis. The result for K Galois over k follows since k is the intersection of the fixed fields of the automorphisms in $\text{Gal}_k(K)$. □

Somewhat similar reasoning may be used to show:

Proposition 2.9. *Let $D : K \rightarrow K$ be a derivation, let $k_D \subset K$ be the kernel of D – i.e. the subfield of D constants – and let $D[X]$ be the extension of D to $K[X]$ by having D act on the coefficients of polynomials. If $D[X]$ carries the ideal I into itself, then the reduced Gröbner basis of I lies in $k_D[X]$.*

Combining Theorem 2.4 with Propositions 2.8 and 2.9 gives:

Corollary 2.10. *a) Under the hypotheses of Prop. 2.8.a, the field of definition of I lies in k_{α} .*

²Note that $\alpha[X]$ is not a K -algebra homomorphism if α is not the identity map. However, if k is a subfield of K lying in the fixed field of α , then $\alpha[X]$ is a k -algebra endomorphism of $K[X]$.

- b) Under the hypotheses of Prop. 2.8.b, the field of definition of I lies in k .
 c) Under the hypotheses of Prop. 2.9, the field of definition of I lies in k_D .

3. SUBALGEBRA COEFFICIENTS

In this section we consider K -subalgebras instead of ideals, and we use the theory of SAGBI (see [RS], [CHV] and [S]). So let $B \subseteq K[X]$ be a K -subalgebra and let σ be a term-order. We recall that σ induces a filtration on $K[X]$, such that the associated graded ring is isomorphic to $K[X]$, graded over \mathbb{N}^n in such a way that

$$K[X]_{(a_1, \dots, a_n)} = \{cX_1^{a_1} \cdots X_n^{a_n} \mid c \in K\}.$$

Moreover, σ induces a filtration \mathcal{F} on the K -subalgebra B , whose associated graded ring $gr_{\mathcal{F}}(B)$ is the monoid K -algebra $K[\text{Lt}_{\sigma}(B)]$, where

$$\text{Lt}_{\sigma}(B) := \{\text{Lt}_{\sigma}(F) \mid F \in B, F \neq 0\}.$$

Definition 3.1. A subset $E = \{F_i \mid i \in S\}$ of B is called a *SAGBI* of B with respect to σ if

$$K[\text{Lt}_{\sigma}(B)] = K[\{\text{Lt}_{\sigma}(E)\}].$$

We recall that if B is finitely generated over K , i.e. there exist F_1, \dots, F_r such that $B = K[F_1, \dots, F_r]$, then B need not have a finite SAGBI.

Example 3.2. For more details see [O], Section 4, and [RS], Examples 1.20 and 4.11. Let $B := K[X, XY - Y^2, XY^2] \subset K[X, Y]$, where K is a field of characteristic 0. If we consider a term-order σ such that $X >_{\sigma} Y$, then $K[\text{Lt}_{\sigma}(B)] = K[X, XY, XY^2, XY^3, XY^4, \dots]$; hence the monoid $\text{Lt}_{\sigma}(B)$ is *not* finitely generated. Instead, if we consider a term-order σ such that $Y >_{\sigma} X$, then $K[\text{Lt}_{\sigma}(B)] = K[X, Y^2, X^2Y]$ is finitely generated.

Let $B := K[X + Y, XY, XY^2] \subset K[X, Y]$, where K is any field. Then $K[\text{Lt}_{\sigma}(B)]$ is not finitely generated for any term order.

Definition 3.3. A K -subalgebra B of $K[X]$ is called σ -finite if it has a finite SAGBI with respect to σ .

Definition 3.4. Let K be a field with subfield L and let B be a K -subalgebra of $K[X]$. B is *defined over* L if B is generated as a K -subalgebra of $K[X]$ by polynomials lying in $L[X]$. It will be shown in Theorem 3.9 that there is a subfield of K over which B is defined and which lies in all other subfields of K over which B is defined. This smallest subfield of K over which B is defined will be referred to as the *field of definition* of B .

The proof that subalgebras have a field of definition parallels the proof of Theorem 2.4. One difficulty is that the proof of Theorem 2.4 relies on reduced Gröbner bases, and the SAGBI analog to reduced Gröbner bases does not yet exist. We remedy this deficiency. It is natural to wonder when fields of definition of subalgebras are finitely generated over the prime field and can be found constructively. We give partial answers to these questions.

Definition 3.5. Let B be a K -subalgebra of $K[X]$ and σ a term-order. Let $E := \{F_i \mid i \in S\}$ be a SAGBI of B with respect to σ . Then E is said to be *subduced* if the lead coefficient of each element of E is 1 and no subduction (subalgebra-reduction) can occur among the F_i 's. This means that neither the lead term of any F_i nor any internal term of an F_i is a scalar from K times a product of lead terms of other F_j 's.

Lemma 3.6. *Let B be a monomial K -subalgebra of $K[X]$.³ Then B has a K -algebra generating set S' consisting of monomials, where S' lies in all other K -algebra generating sets of B consisting of monomials. In fact, if S is any set of monomials which generates B as a K -algebra and 1 does not lie in S , then $S \setminus (S^2 \cup S^3 \cup S^4 \dots)$ is this smallest monomial generating set of B .*

Proof. A simple proof of this known fact goes as follows. Let S be a set of monomials which generates B as a K -algebra. If 1 lies in S , discard it, so all the elements of S have total degree 1 or more. If $b \in B$ has total degree $n > 0$, it is the product of at most n elements of S . The fact that there is such a bound implies that there is a maximal length expression $b = s_1 \dots s_m$ with the s_i 's in S . By the maximality it follows that none of these s_i 's can be expressed as the product of two or more elements of S . Let S' be the subset of S consisting of elements which are not the product of two or more elements of S ; that is, $S' = S \setminus (S^2 \cup S^3 \cup S^4 \dots)$. We have just shown that S' generates B as a K -algebra. By definition, no element of S' is the product of two or more elements of S , and certainly not the product of two or more elements of S' . Hence no element s of S' lies in the K -subalgebra generated by $S' \setminus \{s\}$. Thus S' is a minimal generating set of B .

Next suppose that T is a set of monomials which generates B , and assume that 1 does not lie in T . Let $s' \in S'$. Since T is a monomial generating set, s' lies in $(T \cup T^2 \cup T^3 \dots)$. If $s' \in S'$ were in $(T^2 \cup T^3 \dots)$, i.e. if s' were the product of two or more elements of T (and remember that each of these elements of T are in S' or are the product of elements of S' because S' generates B), then s' is the product of two or more elements of S' . This contradicts the definition of S' . Hence, $s' \in T'$, i.e. $S' \subset T$, and so S' is this smallest monomial generating set of B . \square

Theorem 3.7. *Let B be a K -subalgebra of $K[X]$ and σ a term-order. Then there exists a unique subduced SAGBI of B with respect to σ , which we call E_σ . If B is σ -finite over a constructive field, there is an algorithm to find E_σ .*

Proof. Lemma 3.6 implies that there exists a smallest generating set G of $K[\text{Lt}_\sigma(B)]$ consisting of monomials. Let S be a corresponding SAGBI, i.e. a SAGBI where each element of G is the lead term of a unique element of S . By this construction of S the lead term of any element of S is not a product of the lead terms of other elements of S . For $s \in S$, either no internal terms can be subduced against the other elements of S , or there is a largest, in the term order, internal term of s which can be subduced. In the latter case, subduce this internal term to obtain a new element s' to replace s . s' has the same lead term as s . Now repeat the process with s' . After a finite number of steps this leads to an $s^{(n)}$ to replace s , where $s^{(n)}$ has the same lead term as s and no internal term of $s^{(n)}$ is a product of lead terms of other elements of S . After this "internal subduction" of all the elements of S , one has a subduced SAGBI for B .

Next suppose that S and T are subduced SAGBI's for B . Since S is subduced, the lead terms of S must be a minimal monomial generating sets for $K[\text{Lt}_\sigma(B)]$. Similarly for T . So by Lemma 3.6 for each element of S there is a unique element of T with the same lead term, and vice-versa. Hence S equals T if and only if these corresponding elements with the same leading term are equal. Suppose not.

³By *monomial* we mean an element of $K[X] = k[X_1, \dots, X_n]$ of the form $X_1^{e_1} \dots X_n^{e_n}$. A monomial K -subalgebra is one which is generated by monomials or, equivalently, is spanned by monomials as a vector space over K .

Suppose $s \in S$ and $t \in T$ have the same lead term but are not equal. Consider the non-zero element $s - t$. Because the lead terms of s and t cancel, the lead term of $s - t$ is one of the intermediate terms of s or t . If the lead term of $s - t$ is an intermediate term of s , then it cannot be subduced by elements of S because S is a subduced SAGBI. If the lead term of $s - t$ is an intermediate term of t , then it cannot be subduced by elements of T because T is a subduced SAGBI. Either way we have produced an element of B which cannot be subduced to 0 by a SAGBI, S or T . This contradiction proves that $S = T$.

Note that if B is σ -finite over a constructive field, then the theory of SAGBI's gives an algorithm to construct a finite SAGBI S for B . Exclude constants from S , normalize so that all the lead terms are 1, and where several elements of S have the same lead term keep only one. Next exclude elements of S where the lead term is the product of two or more lead terms of elements of S . Since S is finite, this is a finite check. By Lemma 3.6 the S at this point corresponds to a minimal basis of monomials of $K[\text{Lt}_\sigma(B)]$. Use this S , and internally subduce the elements as in the previous part of the proof. The result, after a finite number of steps, is a subduced SAGBI for B . \square

Example 3.8. Let $B := K[X^3 - Y^2Z, YZ - Z^2]$, $\sigma := \text{DegRevLex}$, i.e. the reverse lexicographic order. Then $\{X^4 - Y^2Z^2, YZ - Z^2\}$ is a SAGBI of B , but it is not subduced because Y^2Z^2 equals $(YZ)^2$ and YZ is the lead term of a SAGBI element. Instead $\{X^4 - Z^4, YZ - Z^2\}$ is the subduced SAGBI.

Now that we have subduced SAGBI's, we can apply them to proving that a subalgebra has a field of definition. Note how the matter of finite generation is more delicate than in the case of ideals.

Theorem 3.9. *Let B be a K -subalgebra of $K[X]$, let σ be a term-order, let E_σ be the subduced SAGBI of B with respect to σ and let k be the subfield of K generated by the coefficients of the polynomials in E_σ .*

- a) B is defined over k , and k lies in all subfields of K over which B is defined.
- b) If B is a finitely generated K -subalgebra of $K[X]$ or there is a subfield L of K where L is a finitely generated field extension of the prime subfield and B is defined over L , then the field of definition of B is finitely generated over the prime subfield.

Proof. a) Again, the coefficients of the polynomials in E_σ are obtained by field operations (addition, subtraction, multiplication and division) on the coefficients of any set of polynomials which generate B as a K -algebra. So the proof proceeds exactly the same as the proof of Theorem 2.4.

b) If B is a finitely generated K -subalgebra of $K[X]$, then let L be the subfield of K generated over the prime field by the coefficients of the generating polynomials of B . There are just a finite number of coefficients for each of the finite number of generating polynomials, and so L is a finitely generated field extension of the prime subfield. Hence it suffices to prove the assertion about B being defined over L , a finitely generated field extension of the prime subfield. Since the field of definition of B is a subfield of L , it follows from ([L93], p.374, ex.4) that the field of definition of B is a finitely generated field extension of the prime subfield. \square

The subalgebra analog to Corollary 2.6 is immediate:

Corollary 3.10. *Let B be a K -subalgebra of $K[X]$. The subfield of K generated over the prime field by the coefficients of E_σ is independent of the term-order.*

Suppose that K is a constructive field and B is finitely generated K -subalgebra. Beginning with a finite generating set of polynomials for B , there is a method to construct increasing finite sets whose union is a SAGBI for B and B is σ -finite if and only if this procedure terminates in a finite number of steps. In this case the procedure is an algorithm for finding a SAGBI for B . The next result is worse than it sounds because one does not have general techniques to ascertain σ -finiteness (in advance).

Corollary 3.11. *Let B be a K -subalgebra of $K[X]$, where K is a constructive field. Suppose that a specific, finite K -algebra generating set for B is given and that B is σ -finite with respect to a term order σ . Then the field of definition of B can be found algorithmically.*

The SAGBI form of Corollary 2.10 holds with about the same proof.

Corollary 3.12. *a) Let $\alpha : K \rightarrow K$ be a homomorphism and let $k_\alpha \subset K$ be the fixed subfield of α . If $\alpha[X]$ carries the K -subalgebra B into itself, then the field of definition of B lies in k_α .*

b) Let K be a Galois extension of k with Galois group $\mathcal{G}al_k(K)$, and suppose that B is a K -subalgebra of $K[X]$ which is stable with respect to $\mathcal{G}al_k(K)[X]$. Then the field of definition of B lies in k .

c) Let $D : K \rightarrow K$ be a derivation and let $k_D \subset K$ be the kernel of D . If $D[X]$ carries the K -subalgebra B into itself, then the field of definition of B lies in k_D .

REFERENCES

- [AL] W. W. Adams, P. Loustau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, American Mathematical Society, Providence RI, 1994. MR **95g**:13025
- [CHV] A. Conca, J. Herzog, G. Valla, *Sagbi Bases with Applications to Blow-up Algebras*, J. Reine Angew. Math. **474**(1996) 113–138. MR **97h**:13023
- [E] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, Springer-Verlag, New York NY, 1995. MR **97a**:13001
- [KM] D. Kapur, K. Madlener, *A completion procedure for computing a canonical basis for a k -subalgebra*, in Computers and Mathematics (Cambridge, MA, 1989), (E. Kaltofen and S. M. Watt, Eds.) pp. 1–11, Springer-Verlag, New York NY, 1989. MR **90g**:13001
- [L58] S. Lang, *Introduction to Algebraic Geometry*, Tracts in Pure and Applied Mathematics, Interscience, New York NY, 1958. MR **20**:7021
- [L93] S. Lang, *Algebra*, Addison-Wesley, Reading MA, 1984. MR **86j**:00003
- [O] F. Ollivier, *Canonical bases: relations with standard bases, finiteness conditions and application to tame automorphisms*, in Effective Methods in Algebraic Geometry (Castiglione-cello, 1990), (T. Mora and C. Traverso, Eds.), pp. 379–400, Progress in Mathematics **94**, Birkhäuser Boston, Boston, MA, 1991. MR **92c**:13026
- [RS] L. Robbiano, M. Sweedler, *Subalgebra bases*, in Commutative Algebra (Salvador, 1988), (W. Bruns and A. Simis, Eds.), pp. 61–87, Lecture Notes in Mathematics **1430**, Springer-Verlag, 1990. MR **91f**:13027
- [S] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series **8**, American Mathematical Society, Providence RI, 1996. MR **97b**:13034
- [T] C. Traverso, *Metodi costruttivi e calcolo automatico in algebra commutativa*, Boll. Un. Mat. Ital. **2–A**(1988) 145–167. MR **89k**:13001

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GENOA, ITALY
E-mail address: robbiano@dimma.unige.it

DEPARTMENT OF MATHEMATICS, CORNELL UNIVERSITY, ITHACA, NEW YORK 14853
E-mail address: moss_sweedler@cornell.edu