Using Groebner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: return of the killer tag variables

Moss Sweedler
ACSyAM / MSI, 409 College Ave
Cornell University
Ithaca NY 14853

ABSTRACT: Suppose I is a prime ideal in $k[X_1, \cdots, X_n]$ with a given finite generating set and $k(q_1,\ldots,q_m)$ is a finitely generated subfield of the field of fractions Z of $k[X_1, \cdots, X_n]/I$ and c is an element of Z. We present Groebner basis techniques to determine:

* if c is transcendental over $k(q_1,\ldots,q_m)$,
* a minimal polynomial for c if c is algebraic over $k(q_1,\ldots,q_m)$.
* the algebraic or transcendental nature of Z over $k(q_1,\ldots,q_m)$.

The information about c also tells whether c lies in $k(q_1,\ldots,q_m)$, solving the subfield membership problem. Determination of the algebraic or transcendental nature of Z over $k(q_1,\ldots,q_m)$ includes finding the index in case of algebraicity or transcendence degree in case the extension is transcendental. The determination of the nature of Z over $k(q_1,\ldots,q_m)$ is not simply an iterative application of the results for c and only requires computing one Groebner basis.

1 INTRODUCTION:

Certain questions about fields reduce to questions about finitely generated commutative algebras. For example, suppose L is a field containing an element c and a subfield K. One may wish to determine if c is algebraic or transcendental over K and if c is algebraic over K, one may wish to determine a minimal polynomial for c over K. Frequently, in computational algebra, L is the field of rational functions in several variables $X_1,\ldots,X_n$, c is given as a rational function and the subfield K is generated - *as a field* - by a given finite set S of rational functions. In this case, there is a *common denominator* D, where c and S lie in the finitely generated algebra A which is generated by the X_i's and $1/D$. The issue of c being transcendental over K reduces to c being transcendental over B, where B is the subalgebra of A which is (*algebra*) generated by S. In section 2 we describe several processes for dealing with this and related situations. Groebner bases are the underlying engine which make both processes run, constructively. *Process one* determines the algebraic or transcendental nature of c over B. The variant - *process two* - determines the algebraic or transcendental nature of A over B in *one shot*, rather than using *process one* repeatedly. Both processes pertain to finitely generated commutative algebras. After the processes are presented, the proofs that the processes perform as promised and application of the processes appear in sections 3 and 4.

Supported in part by NSF & ARO through ACSyAM/MSI at Cornell University, #DAAL03-91-C-0027.

The final application deals with a more general situation than simply subfields of rational function fields. It solves the following problems. Suppose:

I is a prime ideal in $k[X_1, \cdots, X_n]$ with a given finite generating set

$k(q_1,\ldots,q_m)$ is a finitely generated subfield of Z the field of fractions of $k[X_1, \cdots, X_n]/I$

c is an element of Z

Process one may be applied to determine:

* if c is transcendental over $k(q_1,\ldots,q_m)$,
* a minimal polynomial for c if c is algebraic over $k(q_1,\ldots,q_m)$. This also determines if $c \in k(q_1,\ldots,q_m)$.

Process two may be applied to determine the algebraic or transcendental nature of Z over $k(q_1,\ldots,q_m)$. This includes the index in case of algebraicity or transcendence degree in case the extension is transcendental.

CREDITS: In part, this paper deals with transcendence degree. See [Kredel88], [Ollivier89] and [Audoly91] for related work. The source from which this paper springs is [Shannon87]. Dave Shannon is spiritually a joint author of this paper. The subtitle: "Return of the Killer Tag Variables" comes from the fact that [Shannon87], like [Shannon88] and the apocryphal [Spear77], uses tag variables to *knock off* the problem.

2 PROCESSES FOR ALGEBRAS

2.1 THE SETTING: 1. A is a finitely generated commutative algebra over a ground field k and $\{ a_0,\ldots,a_n \}$ is a generating set for A over k. $k[X_0,\ldots,X_n]$ is the polynomial ring in the n variables $\{ X_i \}$ and γ is used to denote the k-algebra map $\gamma: k[X_0,\ldots,X_n] \to A$, $f(X_0,\ldots,X_n) \to f(a_0,\ldots,a_n)$.

2. H_γ is an explicitly given finite subset of $k[X_0,\ldots,X_n]$ which generates the ideal Ker γ.

3. B is a subalgebra of A and B is generated by $\{ b_1,\ldots,b_m \}$.

4. c is an element in A.

5. The b_i's and c are explicitly given as polynomials in the a_i's. I.e. we are given polynomials $B_i(X_0,\ldots,X_n)$ and $C(X_0,\ldots,X_n)$ where $\gamma(B_i) = B_i(a_0,\ldots,a_n) = b_i$ and $\gamma(C) = C(a_0,\ldots,a_n) = c$.

2.2 <u>FIRST CONSTRUCTION:</u> Form the polynomial ring $k[X_0,\ldots,X_n,S,T_1,\ldots,T_m]$. Using any term order where each X_i is greater than any monomial in $k[S,T_1,\ldots,T_m]$ and S is greater than any monomial in $k[T_1,\ldots,T_m]$, construct a Groebner basis G for the ideal generated by:

2.3 $$H_\gamma \cup \{ S - C \} \cup \{ T_i - B_i \}_i$$

Within G let $G_T = G \cap k[T_1,...,T_m]$ and let $G_S = \{ h \in G \cap k[S,T_1,...,T_m]$: the lead term of h is not divisible by the lead term of any element of $G_T \}$.[1]

2.4 FIRST CONCLUSIONS: **a.** If $h \in G_S$, then $h \in k[S,T_1,...,T_m]$ and we consider h to be a polynomial of $S,T_1,...,T_m$; i.e. $h = h(S,T_1,...,T_m)$. $h(S,b_1,...,b_m)$ viewed as a polynomial p(S) in B[S] has the property: p(S) is a non-zero polynomial where $p(c) = 0$. Moreover $\text{degree}_S\, h = \text{degree}_S\, p(S)$.

b. If there exists a non-zero polynomial p(S) in B[S] with $p(c) = 0$ then there is a polynomial h in G_S where $\text{degree}_S\, h \leq \text{degree}_S\, p(S)$.

c. c is integral over B if and only if G contains an element whose lead term is a pure power of S. In this case, the minimal e where G contains an element with lead term S^e is the same as the minimal degree of integral polynomial satisfied by c over B.

d. Suppose A is an integral domain. Let (B) denote the field of fractions of B. c is algebraic over (B) if and only if G_S is non-empty. In this case, let g be a polynomial in G_S of minimal S-degree. Then $p(S) = g(S,b_1,...,b_m)$ is a minimal degree polynomial in B[S] for c over (B).

Although p(S) is not monic in general, part (**d**) shows that the degree of the field extension is $\text{degree}_S\, g$.

2.5 SECOND CONSTRUCTION: Form the polynomial ring $k[X_0,...,X_n,T_1,...,T_m]$. Using any term order where each X_i is greater than any monomial in $k[X_{i+1},...,X_n,T_1,...,T_m]$,[2] construct a Groebner basis G for the ideal generated by:

2.6 $$H_\gamma \cup \{ T_i - B_i \}_i$$

Within G let $G_T = G \cap k[T_1,...,T_m]$ and let $G_i = \{ h \in G \cap k[X_i,...,X_n,T_1,...,T_m]$: the lead term of h is not divisible by the lead term of any element of $G \cap k[X_{i+1},...,X_n,T_1,...,T_m] \}$.[3] For $i = 0,...,n$ if G_i is *not empty* define E_i as the minimal positive integer such that there is h_i in G_i with $\text{degree}_{X^i}\, h_i = E_i$.

2.7 SECOND CONCLUSIONS: Suppose A is an integral domain. Let (A) and (B) denote the respective fields of fractions of A and B.

---

1 If G is a reduced Groebner basis then G_S has a simpler description as $(G \cap k[S,T_1,...T_m]) - G_T$. The somewhat more complicated description eliminates the need for a reduced Groebner basis.

2 "$k[X_j,...,X_n,T_1,...,T_m]$" means "$k[T_1,...,T_m]$" for $j \geq n$.

3 If G is a reduced Groebner basis then, G_i has a simpler description as: $(G \cap k[X_i,...,X_n,T_1,...,T_m]) - k[X_{i+1},...,X_n,T_1,...,T_m]$. The somewhat more complicated description eliminates the need for a reduced Groebner basis.

a. If all the G_i's are non-empty then (A) is algebraic over (B) and the index of the extension is $\Pi_i E_i$.

b. If one of the G_i's is empty then (A) is transcendental over (B) and the transcendence degree of the extension is the number of empty G_i's.

3 VERIFICATION: We continue and extend the notation already developed. Γ is used to denote the algebra map $k[X_0,\dots,X_n,S,T_1,\dots,T_m] \dashrightarrow A$, $f(X_0,\dots,X_n,S,T_1,\dots,T_m) \dashrightarrow f(a_0,\dots,a_n,c,b_1,\dots,b_m)$. Γ extends the previous γ. Let H_Γ denote the set $H_\gamma \cup \{ S - C \} \cup \{ T_i - B_i \}_i$ in (2.3). Recall that $\operatorname{Ker}\gamma$ is generated by H_γ

3.1 LEMMA: $\operatorname{Ker}\Gamma$ is generated by H_Γ.

PROOF: Since $c = C(a_0,\dots,a_n)$ and $b_i = B_i(a_0,\dots,a_n)$ it follows that H_Γ lies in $\operatorname{Ker}\Gamma$. Now to show that H_Γ actually generates $\operatorname{Ker}\Gamma$. Put any term order on $k[X_0,\dots,X_n]$ and with respect to this term order let G_γ be a Groebner basis for the ideal generated by H_γ. Since H_γ and G_γ generate the same ideal, it suffices to prove that $\operatorname{Ker}\Gamma$ is generated by $G_\Gamma = G_\gamma \cup \{ S - C \} \cup \{ T_i - B_i \}_i$.

Extend the term order of the previous paragraph to any term order on $k[X_0,\dots,X_n,S,T_1,\dots,T_m]$ which has the property that S and all T_i's are greater than any monomial in $k[X_0,\dots,X_n]$. We show that G_Γ not only generates $\operatorname{Ker}\Gamma$ but is a Groebner basis for $\operatorname{Ker}\Gamma$. We do this by showing that any element of $\operatorname{Ker}\Gamma$ reduces to zero over G_Γ. Since S is the lead term of $S - C$ and T_i is the lead term of $T_i - B_i$, any polynomial in $k[X_0,\dots,X_n,S,T_1,\dots,T_m]$ reduces over $\{ S - C \} \cup \{ T_i - B_i \}_i$ to a polynomial in $k[X_0,\dots,X_n]$. Since Γ extends γ, $\operatorname{Ker}\Gamma \cap k[X_0,\dots,X_n] = \operatorname{Ker}\gamma$. Hence, reducing any element of $\operatorname{Ker}\Gamma$ over $\{ S - C \} \cup \{ T_i - B_i \}_i$ to an element of $k[X_0,\dots,X_n]$, yields an element of $\operatorname{Ker}\gamma$. This further reduces to zero over G_γ since G_γ is a Groebner basis for $\operatorname{Ker}\gamma$. **QED**

3.2 PROOF of FIRST CONCLUSIONS (2.4): a. Say $h \in G_S$ and form $p(S) = h(S,b_1,\dots,b_m)$ as in (2.4,a). Then $p(c) = h(c,b_1,\dots,b_m) = \Gamma(h)$ and this is zero because h lies in $\operatorname{Ker}\Gamma$. To see that $\operatorname{degree}_S h = \operatorname{degree}_S p(S)$, consider h as a polynomial in $k[T_1,\dots,T_m][S]$. Write h as:

$$h_0(T_1,\dots,T_m)S^e + h_1(T_1,\dots,T_m)S^{e-1} + \dots + h_e(T_1,\dots,T_m)$$

where $h_0(T_1,\dots,T_m)$ is non-zero. The term order in (2.2) has S larger than any monomial in $k[T_1,\dots,T_m]$. Hence the lead term of h is the lead term of $h_0(T_1,\dots,T_m)S^e$ and this is precisely the lead term of h_0 multiplied by S^e. Because h lies in G_S, this lead term is not divisible by any element of G_T. Hence the lead term of h_0 is not divisible by any element of G_T and h_0 does not reduce to zero over G_T.

The choice of term order insures that $G \cap k[T_1,...,T_m] = G_T$ generates $\mathrm{Ker}\,\Gamma \cap k[T_1,...,T_m]$. Hence the fact that h_0 does not reduce to zero over G_T insures that $\Gamma[h_0] = h_0(b_1,...,b_m)$ is non-zero. Thus $p(S) =$

$$h_0(b_1,...,b_m)S^e + h_1(b_1,...,b_m)S^{e-1} + ... + h_e(b_1,...,b_m)$$

is a polynomial of S-degree e in B[S]. This also shows that p(S) is non-zero.

b. Say $p(S)$ is a non-zero polynomial in $B[S]$ with $p(c) = 0$. Write p as $\beta_0 S^e + \beta_1 S^{e-1} + ... + \beta_e$ with β_j's in B and β_0 not equal to zero. Since the b_i's generate B as an algebra, there are polynomials $h_j(T_1,...,T_m)$ where each $\beta_j = h_j(b_1,...,b_m) = \Gamma(h_j)$. Let us assume that $h_0(T_1,...,T_m)$ has been *chosen with minimal lead monomial* among those elements which Γ maps to β_0. Define h in $k[S,T_1,...,T_m]$ by:

$$h = h_0(T_1,...,T_m)S^e + h_1(T_1,...,T_m)S^{e-1} + ... + h_e(T_1,...,T_m)$$

Then $\Gamma(h) = h_0(b_1,...,b_m)c^e + h_1(b_1,...,b_m)c^{e-1} + ... + h_e(b_1,...,b_m) = \beta_0 c^e + \beta_1 c^{e-1} + ... + \beta_e = p(c) = 0$. Hence h lies in $\mathrm{Ker}\,\Gamma$ and so must reduce to zero over the Groebner basis G in (2.2). As in the proof of part **a**, the lead term of h is the lead term of $h_0(T_1,...,T_m)$ times S^e. This lead term must be divisible by (the lead term of) an element g of G since h reduces to zero over G.

We shall show that g lies in G_S. The fact that g divides the lead term of h implies that, $\mathrm{degree}_S\, g \leq = \mathrm{degree}_S\, h = e = \mathrm{degree}_S\, p$. Thus g has the claimed "degree_S" property. The way we show that g lies in G_S is to show that h lies in the set **N** defined by:

$\{ d \in k[S,T_1,...,T_m]$: the lead term of d is not divisible by the lead term of any element of $G_T \}$

If h lies in **N** and the lead term of g divides the lead term of h, then g lies **N** by transitivity of *divisibility*. This shows that g lies in G_S since $G_S = \mathbf{N} \cap G$.

Can the lead term of h be divisible by the lead term of an element of G_T? Suppose so. Suppose there is f in G_T whose lead term divides the lead term of h. Since f lies in $k[T_1,...,T_m]$, it follows that the lead term of f divides the lead term of $h_0(T_1,...,T_m)$. Thus $h_0(T_1,...,T_m)$ reduces over $\{ f \}$ to an element $e_0(T_1,...,T_m)$ with smaller lead term. Since f lies in G which lies in $\mathrm{Ker}\,\Gamma$, $\Gamma(e_0(T_1,...,T_m)) = \Gamma(h_0(T_1,...,T_m))$ which contradicts the minimality property of h_0. Hence h lies in **N** and g lies in G_S.

c. Suppose c is integral over B. Let p(S) in part (**b**) be an integral polynomial. Thus $\beta_0 = 1$ in the proof of part (**b**) above. Follow that proof using 1 for $h_0(T_1,...,T_m)$

when "pulling back" β_0. It then follows that the g, in the proof, has a lead term which is a pure power of S. And as above: $\text{degree}_S\ g \le e = \text{degree}_S\ p$.

Conversely, say g is an element of G whose lead term is a pure power of S. Since the X_i's are greater than all monomials in $k[S,T_1,...,T_m]$ in the term order (2.2), g must lie in $k[S,T_1,...,T_m]$ and hence in G_S. As in the proof of part (a), $g(S,b_1,...,b_m)$ gives a polynomial in $B[S]$ satisfied by v. Moreover, $\text{degree}_S\ g = e = \text{degree}_S\ g(S,b_1,...,b_m)$. Finally, note that $g(S,b_1,...,b_m)$ is a monic polynomial in $B[S]$.

d. If h lies in G_S then part (a) shows that $p(S) = h(S,b_1,...,b_m)$ gives a polynomial satisfied by c over B and hence (B). Moreover part (a) gives: $\text{degree}_S\ h = \text{degree}_S\ p(S)$. Conversely, assume c is algebraic over (B), let q(S) be a minimal degree polynomial for c over (B). Since the coefficients of q lie in (B) there is a common denominator b in B where bq has coefficients in B. I.e. $p = bq$ is a polynomial in $B[S]$, of same S-degree as q, satisfied by c. By part (b), G_S contains an element of this S-degree or less. **QED**

3.3 PROOF of SECOND CONCLUSIONS (2.7): The trick here is to view the information produced by the second construction (2.5) from $n+1$ points of view and each time apply the first conclusion. To be more precise, for $i = 0,...,n$.

VIEW i: $c_i = a_i$, $B_i = k[a_{i+1},...,a_n,b_1,...,b_m]$. In this view X_i plays the role of S in the first process; $X_{i+1},...,X_n,T_1,...,T_m$ plays the role of $T_1,...,T_m$ in the first process and G_i plays the role of G_S in the first process.

The tower of algebras $B_0 \supset B_1 \supset ... \supset B_n \supset B$ gives the tower of fields $(B_0) \supset (B_1) \supset ... \supset (B_n) \supset (B)$. The rest is a straightforward $n+1$ fold application of (2.4) and standard results about algebraicity and transcendentality of towers of fields. **QED**

4 FIELD APPLICATIONS:

4.1 APPLICATION TO FIELDS OF RATIONAL FUNCTIONS AND FINITELY GENERATED SUBFIELDS: The first application is to finitely generated subfields of the field of rational functions: $k(Y_1,...,Y_n)$. Suppose $k(q_1,...,q_m)$ is a finitely generated subfield of $k(Y_1,...,Y_n)$, where $q_i \in k(Y_1,...,Y_n)$. Furthermore, let c be an element of $k(Y_1,...,Y_n)$. Find a common denominator $d \in k[Y_1,...,Y_n]$ where $dq_i \in k[Y_1,...,Y_n]$, $dc \in k[Y_1,...,Y_n]$ and let p_i denote dq_i and let C denote dc. Let A be the subalgebra of $k(Y_1,...,Y_n)$ generated by $\{1/d, Y_1,...,Y_n\}$ and let B be the subalgebra of A generated by $\{p_1/d,...,p_m/d\}$. Note that $c = C/d$ also lies in A. Consider the map $\gamma: k[X_0,X_1,...,X_n] \text{-->} A$, $f(X_0,X_1,...,X_n) \text{-->} f(1/d,Y_1,...,Y_n)$. It is well known and easy to verify that $\text{Ker}\,\gamma$ is generated by $X_0 d(X_1,...,X_n) - 1$. (Originally d is a polynomial in $k[Y_1,...,Y_n]$

and we are substituting X's for the Y's.) Hence, let $H_\gamma = \{ X_0 - d(X_1,...,X_n) \}$. Finally note that $(A) = k(Y_1,...,Y_n)$ and $(B) = k(q_1,...,q_m)$.

Process one may be applied to determine:

* if c is transcendental over $k(q_1,...,q_m)$,
* a minimal polynomial for c if c is algebraic over $k(q_1,...,q_m)$. This also determines if $c \in k(q_1,...,q_m)$.

Process two may be applied to determine the algebraic or transcendental nature of $k(Y_1,...,Y_n)$ over $k(q_1,...,q_m)$. This includes the index in case of algebraicity or transcendence degree in case the extension is transcendental.

4.2 COMMENTS: If one just wants to learn the nature of the field extension $k(Y_1,...,Y_n)$ over $k(q_1,...,q_m)$ then there is no element **c** and **d** is just the common denominator for $q_1,...,q_m$. Also, if $d = 1$, i.e. the q_i's and c - if there is a c - are all polynomials, then drop d and X_0. I.e. let A be the subalgebra $k[Y_1,...,Y_n]$ of $k(Y_1,...,Y_n)$ and let B be the subalgebra of A generated by $\{ q_1,...,q_m \}$. c - if there is a c - lies in A. The map γ:$k[X_1,...,X_n] \dashrightarrow A$ is determined by:

$$f(X_1,...,X_n) \dashrightarrow f(Y_1,...,Y_n)$$

and $\text{Ker}\,\gamma = \{ 0 \}$. Let H_γ be the empty set.

4.3 LEMMA: Suppose A is a subalgebra of a larger algebra and d is an element of A which is invertible in the larger algebra. Let A[1/d] denote the subalgebra of the larger algebra which is generated by A and 1/d. Let μ:$A[X] \dashrightarrow A[1/d]$ be the algebra map which sends $f(X) \dashrightarrow f(1/d)$. μ maps A[X] onto A[1/d] and has kernel generated by $dX - 1$.

PROOF: Clearly $< dX - 1 >$ lies in the kernel of μ. The opposite inclusion is verified by a little computation. Let $f(X) = a_0X^e + a_1X^{e-1} + \cdots + a_e$ be a polynomial which lies in $\text{Ker}\,\mu$. If $e = 0$, i.e. f has degree zero, then f must be the zero polynomial which lies in $< dX - 1 >$. Hence we may assume that $e \geq 1$. Rewrite f(X) as:

$$(a_0 + a_1d^1 + \cdots + a_ed^e) X^e - (a_1d^1 + \cdots + a_ed^e) X^e + a_1X^{e-1} + \cdots + a_e$$

$0 = f(1/d)$ gives $0 = d^ef(1/d)$ which gives: $0 = a_0 + a_1d^1 + \cdots + a_ed^e$.

Thus the first expression in the rewritten f(X) vanishes, leaving f(X) as:

$$- (a_1d^1 + \cdots + a_ed^e) X^e + a_1X^{e-1} + \cdots + a_e$$

Again, regroup and rewrite, giving f(X) as:

$$a_1 (1 - dX) X^{e-1} + a_2 (1 - (dX)^2) X^{e-2} + \cdots + a_e (1 - (dX)^e)$$

Each $1 - (dX)^i$ equals $1 + dX + \cdots + (dX)^{i-1}$ times $1 - dX$. Hence, f(X) lies in $< dX - 1 >$.

QED

4.4 COROLLARY: Suppose Z is an algebra and the algebra map:

$$\mu{:}k[X_1, \cdots, X_n] \dashrightarrow Z\,,\ f(X_1, \cdots, X_n) \dashrightarrow f(z_1, \cdots, z_n)$$

has kernel generated by the finite set H_μ. Let $d_1, \cdots, d_m$ be elements in the image of μ which are invertible in Z. Choose polynomials $D_1, \cdots, D_m$ in $k[X_1, \cdots, X_n]$ where $\mu(D_i) = d_i$ and consider the algebra map:

$$\gamma{:}k[W_1, \cdots, W_m, X_1, \cdots, X_n] \dashrightarrow Z$$

$$f(W_1, \cdots, W_m, X_1, \cdots, X_n) \dashrightarrow f(1/d_1, \cdots, 1/d_m, z_1, \cdots, z_n)$$

Then $\operatorname{Ker}\gamma$ is generated by:

$$H_\mu \cup \{ D_1W_1 - 1, \cdots, D_mW_m - 1 \}$$

PROOF: The map γ factors into the two maps:

$$k[W_1, \cdots, W_m, X_1, \cdots, X_n] \dashrightarrow Z[W_1, \cdots, W_m] \dashrightarrow Z$$

$$f(W_1, \cdots, W_m, X_1, \cdots, X_n) \dashrightarrow f(W_1, \cdots, W_m, z_1, \cdots, z_n)$$

$$\dashrightarrow f(1/d_1, \cdots, 1/d_m, z_1, \cdots, z_n)$$

The kernel of the first map is $\operatorname{Ker}\mu$ extended to $k[W_1, \cdots, W_m, X_1, \cdots, X_n]$. Hence it is generated by H_μ. The first map carries $\{ D_1W_1 - 1, \cdots, D_mW_m - 1 \}$ to $\{ d_1W_1 - 1, \cdots, d_mW_m - 1 \}$ which, by the preceding lemma iterated, generates the kernel of the second map. Hence the kernel of the composite - and the composite equals γ - is generated by the given set. **QED**

4.5 APPLICATION TO FINITELY GENERATED FIELDS OVER FINITELY GENERATED SUBFIELDS: Suppose I is a prime ideal in $k[X_1, \cdots, X_n]$ with finite generating set H_I. Let P denote $k[X_1, \cdots, X_n]/I$ and let:

$$\mu{:}k[X_1, \cdots, X_n] \dashrightarrow P$$

be the natural algebra map. Z denotes the field of fractions of P. If $z_i = \mu(X_i)$, then μ may alternatively be described by:

$$f(X_1, \cdots, X_n) \dashrightarrow f(z_1, \cdots, z_n)$$

Suppose we are given a finitely generated subfield $k(q_1, \cdots, q_m)$ of Z and (possibly) an element $c \in Z$. Each q_i and c can be expressed as a quotient $q_i = p_i/d_i$, and $c = p_0/d_0$ with p_i and d_i in P. Let A be the subalgebra of Z generated by P and $\{ 1/d_i \}$. Note that $Z = (A)$. Select D_i in $k[X_1, \cdots, X_n]$ where $\mu(D_i) = d_i$. By the preceding corollary:

$$H_I \cup \{ D_0W_0 - 1, \cdots, D_mW_m - 1 \}$$

generates the kernel of the algebra map:

$$\gamma{:}k[W_0, \cdots, W_m, X_1, \cdots, X_n] \dashrightarrow A$$

$$f(W_0, \cdots, W_m, X_1, \cdots, X_n) \dashrightarrow f(d_0, \cdots, d_m, z_1, \cdots, z_n)$$

Let H_γ denote $H_I \cup \{ D_0W_0 - 1, \cdots, D_mW_m - 1 \}$ and let B be the subalgebra of A generated by $\{ p_i/d_i \}$ so that $k(q_1, \cdots, q_m) = (B)$. Modulo the renaming $X_0 \cdots, X_n$ to $W_0, \cdots, W_m, X_1, \cdots, X_n$, the techniques of section 2 now apply.
Process one may be applied to determine:

* if c is transcendental over $k(q_1,...,q_m)$,
* a minimal polynomial for c if c is algebraic over $k(q_1,...,q_m)$. This also determines if $c \in k(q_1,...,q_m)$.

Process two may be applied to determine the algebraic or transcendental nature of Z over $k(q_1,...,q_m)$. This includes the index in case of algebraicity or transcendence degree in case the extension is transcendental.

4.6 COMMENTS: If one just wants to learn the nature of the field extension Z over $k(q_1,...,q_m)$ then there is no element **c** and this permits one to drop W_0. If the q_i's - and c if there is one - actually lie in P, then none of the W_i's are necessary and $A = P$. In (4.1) we found a common denominator and in (4.5) we threw in each denominator separately. Throwing in each denominator separately adds more variables: $W_0, \cdots, W_m$. Finding a common denominator increases the degree of D. One could even do mixed cases, throwing in several partial common denominators. We do not know the best strategy to follow.

REFERENCES:

Audoly,S Bellu,G. Buttu,A and D'Angio',L. (1991). Procedures to investigate injectivity of polynomial maps and to compute the inverse, Lournal Applicable Algebra, 2 91-104

Buchberger,B. (1965). An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal, Dissertation, Universitaet Innsbruck, Institut fuer Mathematik.

Buchberger,B. (1970). An algorithmic criterion for the solvability of algebraic systems of equations. Aequationes Mathematicae 4/3, 374-383.

Buchberger,B. (1976). A theoretical basis for the reduction of polynomials to canonical forms. ACM Sigsam Bull. 10/3 19-29 1976 & ACM Sigsam Bull. 10/4 19-24.

Buchberger,B. (1979). A criterion for detecting unnecessary reductions in the construction of Groebner bases. Proc. of EUROSAM 79, Lect. Notes in Computer Science 72, Springer 3-21.

Buchberger,B. (1984). A critical-pair/completion algorithm for finitely generated ideals in rings. Decision Problems and Complexity. (Proc of the Symposium "Rekursive Kombinatorik", Muenster, 1983.) E. Boerger, G. Hasenjaeger, D. Roedding, eds. Springer Lecture Notes in Computer Science, 171, page 137.

Buchberger,B. (1985). Groebner bases: an algorithmic method in polynomial ideal theory. Multidimensional Systems Theory. N. K. Boese ed. D. Reidel Pub Co. 184-232.

Kredel,H. and Weispfenning, V. (1988). Computing dimension and independent sets for polynomial ideals. Special Volume of the JSC on the computational aspects of commutative algebra. Vol. 6 1988.

Ollivier,F. (1989). Inversibility of rational mappings and structural identifiabily in automatics. Proc. ISSAC' 89, 43-53, ACM

Shannon,D. and Sweedler,M. (1988). Using Groebner bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence. J. Symbolic Computation, 6, 267-273.

Shannon,D. and Sweedler,M. (1987). Using Groebner bases to determine the algebraic or transcendental nature of field extensions within the field of rational functions. Preprint.

Spear,D. (1977). A constructive approach to commutative ring theory. Proceedings 1977 MACSYMA User's Conference, pp.369-376.