Computation of Unirational Fields [1]

Jaime Gutierrez [a,*] David Sevilla [b]

[a] *Faculty of Science, University of Cantabria, E-39071 Santander, Spain*

[b] *Concordia University, Montreal, Canada*

Abstract

One of the main contributions which Volker Weispfenning made to mathematics is related to Gröbner bases theory. In this paper we present an algorithm for computing all algebraic intermediate subfields in a separably generated unirational field extension (which in particular includes the zero characteristic case). One of the main tools is Gröbner bases theory. Our algorithm also requires computing primitive elements and factoring over algebraic extensions. Moreover, the method can be extended to finitely generated $\mathbb{K}$-algebras.

Key words:
Unirational fields, Gröbner Basis, Polynomial and rational function decomposition, Galois theory computational, Lüroth's theorem.

1 Introduction

The goal of this paper is to study the problem of computing intermediate fields between a rational function field and a given subfield of it. Rational function fields arise in various contexts within mathematics and computer science. Two examples are the factorization of regular maps in algebraic geometry (Shafarevich, 1977) and the reparametrization of parametric varieties in computer aided geometric design (Alonso, Gutierrez and Rubio, 1999).

* Corresponding author.
Email addresses: `jaime.gutierrez@unican.es` (Jaime Gutierrez), `davidsevillaglez@yahoo.es` (David Sevilla).

[1] Partially supported by Spain's Ministerio de Educación Grant Project BFM2001-1294 and MTM2004-07086

The question of the structure of the lattice of such intermediate fields is of theoretical interest by itself; we will focus on the computational aspects, like deciding if there are proper intermediate fields and computing them in the affirmative case.

In the univariate case, the problem can be stated as follows: given an arbitrary field $\mathbb{K}$ and $f_1, \ldots, f_m \in \mathbb{K}(t)$, find a field $\mathbb{F}$ such that $\mathbb{K}(f_1, \ldots, f_m) \subsetneq \mathbb{F} \subsetneq \mathbb{K}(t)$. By Lüroth's Theorem, see (van der Waerden, 1964), or (Schinzel, 1982) for a constructive proof by Netto, there exist functions $f, h \in \mathbb{K}(t)$ such that $\mathbb{K}(f_1, \ldots, f_m) = \mathbb{K}(f)$ and $\mathbb{F} = \mathbb{K}(h)$. Therefore, our problem is equivalent to decomposing the rational function f, that is, to find $g, h \in \mathbb{K}(t)$ with deg g, deg $h > 1$ such that $f = g(h)$. Algorithms for decomposition of univariate rational functions can be found in (Zippel, 1991) and (Alonso, Gutierrez and Recio, 1995).

We denote by $\mathbb{K}$ an arbitrary field and by $\mathbb{K}(x_1, \ldots, x_n) = \mathbb{K}(\mathbf{x})$ the rational function field in the variables $\mathbf{x} = (x_1, \ldots, x_n)$. In the multivariate case, the problem can be stated as:

Problem 1 *Given rational functions $f_1, \ldots, f_m \in \mathbb{K}(\mathbf{x})$, compute a proper unirational field $\mathbb{F}$ between $\mathbb{K}(f_1, \ldots, f_m)$ and $\mathbb{K}(\mathbf{x})$, if it exists.*

A *unirational* field over $\mathbb{K}$ is an intermediate field $\mathbb{F}$ between $\mathbb{K}$ and $\mathbb{K}(\mathbf{x})$. We know that any unirational field is finitely generated over $\mathbb{K}$, see (Nagata, 1993). Thus, by computing an intermediate field we mean that such a finite set of generators is to be calculated.

Regarding algorithms for this problem, see (Müller-Quade and Steinwandt, 1999), where the authors generalize the method of (Alonso, Gutierrez and Recio, 1995) to several variables, by converting this problem into the calculation of a primary ideal decomposition. Primary ideal decomposition can be computed by Gröbner bases. The book (Becker and Weispfenning, 1993) is an excellent reference guide to this important theory and its applications. Once the primary ideal decomposition is computed in a polynomial ring with $2n$ variables, their algorithm requires to check a exponential number of generators of the possible intermediate proper subfields — although authors do not study its complexity in detail. On the other hand, the solution is trivial and uninteresting for most choices of $f_1, \ldots, f_m$, since it is easy to construct infinitely many intermediate fields when the transcendence degree of $\mathbb{K}(f_1, \ldots, f_m)$ over $\mathbb{K}$ is smaller than n, as the next theorem shows.

Theorem 1 *If $n >$ tr.deg.$(\mathbb{K}(f_1, \ldots, f_m)/\mathbb{K})$, there exist infinitely many different fields between $\mathbb{K}(f_1, \ldots, f_m)$ and $\mathbb{K}(\mathbf{x})$.*

Proof: At least one of $x_1, \ldots, x_n$ is transcendental over $\mathbb{K}(f_1, \ldots, f_m)$, let us assume that x_1 is. Then the fields

$$\mathbb{K}(f_1,\ldots,f_m,x_1^k)\ ,\quad k\in\mathbb{N}$$

form an infinite set of different intermediate fields. Indeed, if i divides j,

$$\mathbb{K}(f_1,\ldots,f_m,x_1^j)\subsetneq\mathbb{K}(f_1,\ldots,f_m,x_1^i).$$

It is clear that one field is contained in the other. To prove that they are not equal, assume that $x_1^i\in\mathbb{K}(f_1,\ldots,f_m,x_1^j)$. Then there exists a rational function $h(t)$ such that $x_1^i=h(x_1^j)$ where $h\in\mathbb{K}(f_1,\ldots,f_m,t)$ but $h\notin\mathbb{K}(t)$. Then we have the polynomial relation

$$x_1^i\cdot h_D(f_1,\ldots,f_m,x_1^j)-h_N(f_1,\ldots,f_m,x_1^j)=0,$$

(where h_N, h_D denote the numerator and denominator of h resp.) which contradicts x_1 being transcendental over $\mathbb{K}(f_1,\ldots,f_m)$. ■

Due to this result, we will focus on the following version of the problem.

Problem 2 *Given functions $f_1,\ldots,f_m\in\mathbb{K}(\mathbf{x})$, find all the fields $\mathbb{F}$ between $\mathbb{K}(f_1,\ldots,f_m)$ and $\mathbb{K}(\mathbf{x})$ that are algebraic over $\mathbb{K}(f_1,\ldots,f_m)$.*

First, we will prove that there are finitely many algebraic intermediate fields if the original extension is separable. The notion of separable extension can be generalized to non-algebraic extensions. In transcendental extensions, separability means that any finitely generated subfield $\mathbb{F}$ over $\mathbb{K}$ has a separating basis, that is, a transcendence basis B such that $\mathbb{K}(B)\subset\mathbb{F}$ is an algebraic separable extension. The following is a well known result, see for instance (Lang, 1967).

Proposition 1 *The field extension $\mathbb{K}\subset\mathbb{K}(\mathbf{x})$ is separable.*

In general, if $\mathbb{K}'$ is a separable extension of $\mathbb{K}$, then every field between $\mathbb{K}$ and $\mathbb{K}'$ is separable over $\mathbb{K}$. Details on separability and a proof of these results can be found in Nagata (1993) and Lang (1967).

As we said, any unirational field is finitely generated over $\mathbb{K}$. The following result provides a bound for the number of generators and it is known for zero characteristic field. Our algorithm always returns this bound as the number of generators.

Theorem 2 *Let $\mathbb{F}$ be a unirational field such that $\mathbb{K}\subsetneq\mathbb{F}\subset\mathbb{K}(\mathbf{x})$ and $d=$ tr.deg.$(\mathbb{F}/\mathbb{K})$. Then there exist $h_1,\ldots,h_s\in\mathbb{K}(\mathbf{x})$ such that $\mathbb{F}=\mathbb{K}(h_1,\ldots,h_s)$*

and $s \leq d+1$.

Proof: By Proposition 1 we have $\mathbb{K} \subset \mathbb{K}(\mathbf{x})$ is separable, that is, for each subfield $\mathbb{F}$ in $\mathbb{K} \subset \mathbb{K}(\mathbf{x})$ there exists a transcendence basis $\{h_1, \ldots, h_d\}$ of $\mathbb{F}$ over $\mathbb{K}$ such that $\mathbb{K}(h_1, \ldots, h_d) \subset \mathbb{F}$ is algebraic separable. Then, the result follows by the Primitive Element Theorem. ■

Because of the previous results we have the following theorem.

Theorem 3 *If the extension* $\mathbb{K}(\mathbf{x})/\mathbb{K}(f_1, \ldots, f_m)$ *is separable then there exist finitely many intermediate fields that are algebraic over* $\mathbb{K}(f_1, \ldots, f_m)$.

Proof: Let $\mathbb{F}_0$ be the minimum subfield of $\mathbb{K}(\mathbf{x})$ that contains all algebraic intermediate fields. $\mathbb{F}_0$ is clearly algebraic over $\mathbb{K}(f_1, \ldots, f_m)$, and due to the previous theorem the extension $\mathbb{F}_0/\mathbb{K}(f_1, \ldots, f_m)$ is separable. On the other hand, since $\mathbb{F}_0$ is a unirational field is finitely generated over $\mathbb{K}$, see Theorem 2. Therefore, because of the Primitive Element Theorem the extension is simple and there are finitely many fields between $\mathbb{K}(f_1, \ldots, f_m)$ and $\mathbb{F}_0$. ■

Problem 2 for transcendence degree of $\mathbb{K}(f_1, \ldots, f_m)/\mathbb{K}$ is 1 has been treated in (Gutierrez, Rubio and Sevilla, 2001). In this case a generalization of the classical Lüroth's Theorem applies:

Extended Lüroth's Theorem Let $\mathbb{F}$ be a field such that $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(x_1, \ldots, x_n)$ and tr.deg.$(\mathbb{F}/\mathbb{K}) = 1$. Then there exists $f \in \mathbb{K}(x_1, \ldots, x_n)$ such that $\mathbb{F} = \mathbb{K}(f)$. Also, if the field contains a polynomial, then a polynomial generator exists.

By the Extended Lüroth's Theorem, the problem is equivalent to the following: given $f \in \mathbb{K}(\mathbf{x})$, find $g \in \mathbb{K}(y)$ and $h \in \mathbb{K}(\mathbf{x})$ with deg g, deg $h > 1$ such that $f = g(h)$. The paper (Gutierrez, Rubio and Sevilla, 2002) provides a very efficient constructive proof of the above result and it also contains different decomposition algorithms for multivariate rational functions. In some sense, Problem 2 can be seen as a generalization of the univariate rational function decomposition problem.

In this paper we will combine several techniques of computational algebra to create an algorithm that finds all the intermediate fields that are algebraic over the smaller field. Moreover, our method can be extended to finitely generated $\mathbb{K}$-algebras, that is, the case where the ambient field is $\mathbb{K}(z_1, \ldots, z_n) = \mathbb{K}(\mathbf{z})$ for some $z_1, \ldots, z_n$ transcendental over $\mathbb{K}$ (that need not be algebraically independent), and $\mathbb{K}(\mathbf{z})$ is the quotient field of a polynomial ring, so that we have

$$\mathbb{K}(\mathbf{z}) = QF\left(\mathbb{K}[\mathbf{x}]/I\right)$$

(where QF denotes the quotient field of a domain) for some prime ideal $I \subset \mathbb{K}[\mathbf{x}]$ that will be given explicitly by means of a finite system of generators. Unsurprisingly, the algorithm will be much simpler when $\mathbb{K}(\mathbf{x})$ is rational, that is, when $I = (0)$.

The paper is organized as follows. In Section 2 we introduce several algebraic tools in order to manipulate fields and the elements in them. Section 3 is devoted to the algebraic case, and in Section 4 the general case is reduced to it, also other approaches to this are given. Section 5 briefly describes the adaptation of the algorithm to $\mathbb{K}$-algebras. Finally, in Section 6 we summarize the main conclusions of this research and consider some open problems.

2 Algebraic tools

In this section we will introduce several techniques and tools of general interest for the manipulation of fields and functions.

Notation. Through this paper, we will denote the numerator and denominator of a rational function f as f_N and f_D respectively.

2.1 Membership problem

As we have to manipulate function fields and field extensions, we may need to compute generators and elements with certain properties, or to check whether certain functions belong to a given field. The next theorem provides a way to do this. See (Sweedler, 1993) and for more details, see also (Becker and Weispfenning, 1993).

We will use the following notation: Let A be a commutative $\mathbb{K}$-algebra and $\{a_0, \ldots, a_n\}$ be a set of generators of A over $\mathbb{K}$. Let $\mathbb{K}[x_0, \ldots, x_n]$ be a ring of polynomials and

$$\begin{array}{rcl} \gamma : \mathbb{K}[x_0, \ldots, x_n] & \longrightarrow & A \\ f(x_0, \ldots, x_n) & \rightarrow & f(a_0, \ldots, a_n) \end{array}$$

Let H_γ be a finite subset of $\mathbb{K}[x_0, \ldots, x_n]$ which generates Ker γ. Let B be a subalgebra of A and $\{b_1, \ldots, b_m\}$ a set of generators of B given as polynomials $B_i \in \mathbb{K}[x_0, \ldots, x_n]$ such that $\gamma(B_i) = b_i$. Let c be an element of A given as a polynomial $C \in \mathbb{K}[x_0, \ldots, x_n]$ such that $\gamma(C) = c$.

Theorem 4

(i) *If A is an integral domain, given the field extension $QF(A)/QF(B)$ it is possible to decide whether it is transcendental or algebraic and:*

- *if it is transcendental, its transcendence degree can be computed;*
- *if it is algebraic, its degree can be computed.*

(ii) *It is possible to decide whether c is integral over B, and whether c is algebraic over $QF(B)$ and:*

- *if it is algebraic, its minimum polynomial can be computed;*
- *in particular, we can determine whether $c \in QF(B)$ and in the affirmative case we can find an expression of c in terms of b_i.*

This theorem, which is stated for $\mathbb{K}$-algebras, has a simpler form when our ambient field is rational.

Corollary 1 *We can compute transcendence and algebraic degrees of unirational fields, decide whether an element is transcendental or algebraic over a field, compute its minimum polynomial in the latter case, and decide membership.*

We illustrate this corollary with the following example:

Example 1 *Consider the rational functions f_1, f_2 in $\mathbb{Q}(x, y)$, where*

$$f_1 = -y^2x - y^4 + 2\,x + 2\,y^2 - 1,\ \ f_2 = 4\,y^4 - 10\,y^2 + 5 + 3\,y^2x - 6\,x.$$

We want to know if the field extension $\mathbb{Q}(x, y)/\mathbb{Q}(f_1, f_2)$ is algebraic or transcendental, and the corresponding degree in each case. We compute a Gröbner basis G of the ideal $I = (t_1 - f_1, t_2 - f_2) \subset \mathbb{Q}[x, y, t_1, t_2]$ with respect to a tag monomial ordering $\{x, y\} > \{t_1, t_2\}$:

$$\begin{aligned} G = \{&-3\,t_1 + y^4 - 4\,y^2 + 2 - t_2, \\ &3\,xt_1 + xt_2 + 2\,x + 4\,y^2t_1 + y^2t_2 + 3\,y^2 - 2\,t_1 - 2, \\ &y^2x - 2\,x + 2\,y^2 + 4\,t_1 + t_2 - 1\}. \end{aligned}$$

so the transcendence degree is 2, because there is no polynomial involving only t_1, t_2.

On the other hand, the extension is algebraic of degree $4 = 4 \times 1$. The polynomial $-3\,t_1 + y^4 - 4\,y^2 + 2 - t_2$ in G indicates that y is algebraic over $\mathbb{Q}(f_1, f_2)$

and its minimum polynomial $z^4 + z^2 - 3f_1 - f_2 + 2$ *has degree* 4.

Alternatively, a different Gröbner basis computed with respect to lex ordering with $y > x > t_1 > t_2$ *is*

$$\{12\,xt_1 - 16\,{t_1}^2 - 8\,t_1\,t_2 - 12\,t_1 + 3\,x^2t_1 + x^2t_2 + 2\,x^2 + 8\,x + 4\,xt_2 - {t_2}^2 - 2\,t_2 - 1,$$
$$3\,xt_1 + xt_2 + 2\,x + 4\,y^2t_1 + y^2t_2 + 3\,y^2 - 2\,t_1 - 2,\ -3\,t_1 + y^4 - 4\,y^2 + 2 - t_2,$$
$$y^2x - 2\,x + 2\,y^2 + 4\,t_1 + t_2 - 1,\ -3\,t_1 + y^4 - 4\,y^2 + 2 - t_2\}$$

so x *is algebraic over* $\mathbb{Q}(f_1, f_2)$ *and its minimum polynomial has degree 2.*

The computations described in these theorems require Gröbner bases computation with respect tag orderings, thus the computing time is (double) exponential in the number of variables and polynomial in the degree of $f_1, \ldots, f_m$.

2.2 Computation of separating bases

The results that we describe now will allow us to compute a separable basis and the transcendence degree of a separable extension without computing Gröbner bases, greatly increasing the efficiency of our computations. See (Weil, 1946) and (Steinwandt, 2000) for more details about these techniques.

Let $\mathbb{F} = \mathbb{K}(g_1, \ldots, g_m)$ be a unirational field, $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$. First introduce a classical definition that will be very useful for our purpose, see (Weil, 1946).

Definition 1 *Given a field extension* $\mathbb{K}(\mathbf{x})/\mathbb{F}$*, we construct the ring homomorphism* $\phi_{\mathbb{F}} : \mathbb{F}[\mathbf{y}] \longrightarrow \mathbb{K}(\mathbf{x})$ *defined as* $\phi_{\mathbb{F}}(y_i) = x_i$*, where* $\mathbf{y} = (y_1, \ldots, y_n)$*. Its kernel, which we will denote as* $\mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{F}}$*, is called the* ideal of relations *of the extension* $\mathbb{K}(\mathbf{x})/\mathbb{F}$*.*

The paper (Müller-Quade and Steinwandt, 1999) presents a method to find explicit generators of the ideal by means of Gröbner bases techniques. Because of this, the following theorem is fundamental, as it allows to express a related ideal (namely, the extension of our ideal in a certain ring) in a very simple way.

We denote by $\mathbb{F}[\mathbf{y}]_{\mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{F}}}$ the localization ring of $\mathbb{F}[\mathbf{y}]$ at the prime ideal $\mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{F}}$. Let $\mathcal{B}^e_{\mathbb{K}(\mathbf{x})/\mathbb{F}}$ be the extended ideal of $\mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{F}}$ in the local ring $\mathbb{F}[\mathbf{y}]_{\mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{F}}}$, (Atiyah and MacDonald, 1969).

Proposition 2 *With the above notation, we have*

$$\mathcal{B}^e_{\mathbb{K}(\mathbf{x})/\mathbb{F}} = \langle g_1(\mathbf{y}) - g_1(\mathbf{x}), \ldots, g_m(\mathbf{y}) - g_m(\mathbf{x})\rangle.$$

This result can be combined with the next Theorem to provide a relatively fast way to compute transcendence degrees of separable extensions.

Theorem 5 *Let* $C = \{p_l = g_l(\mathbf{y}) - g_l(\mathbf{x}), \quad l = 1, \ldots, m\}$ *and* $t = \mathrm{tr.deg.}(\mathbb{K}(\mathbf{x})/\mathbb{F})$. *Then*

$$\operatorname{rank}\left(\frac{\partial p_i}{\partial y_j}(\mathbf{x})\right)_{p_i \in C, j=1,\ldots,n} \leq n - t$$

and they are equal if and only if $\mathbb{K}(\mathbf{x})/\mathbb{F}$ *is separable.*

Corollary 2 *With the notations of the previous theorem, if* $I \subset C$ *and* $J \subset \{1, \ldots, n\}$ *are such that* $\sharp I = \sharp J = n - t$ *and*

$$\det\left(\frac{\partial p_i}{\partial y_j}(\mathbf{x})\right)_{p_i \in I, j \in J} \neq 0,$$

then the set $\{x_i : \ i \notin J\}$ *is a transcendence basis of* $\mathbb{K}(\mathbf{x})/\mathbb{F}$.

We illustrate this with the following example.

Example 2 *Let*

$$h_1 = \frac{x_1 + x_2 - 2\,x_3}{1 + x_3 x_2}, \ h_2 = \frac{x_1 x_2 - x_3}{x_1} \in \mathbb{Q}(x_1, x_2, x_3).$$

We construct the field $\mathbb{Q}(g_1, g_2, g_3, g_4)$ *where*

$$\begin{aligned}
g_1 &= \frac{x_1^2 x_2 + x_1 x_2^2 - 3\,x_1 x_2 x_3 - x_3 x_1 - x_3 x_2 + 2\,x_3^2 - x_1}{x_1^2 + x_1 x_2 - 2\,x_3 x_1} = h_2 - \frac{1}{h_1},\\
g_2 &= \frac{x_1^2 x_2 + x_1 x_2^2 - 2\,x_1 x_2 x_3 - x_3 x_1 - x_3 x_2 + 2\,x_3^2}{x_1 + x_1 x_2 x_3} = h_1 h_2,\\
g_3 &= \frac{x_1^2 - x_1 x_2 - 2\,x_3 x_1 + 2\,x_3 - 2\,x_3 x_2^2 x_1 + 2\,x_3^2 x_1}{x_1 x_2 - x_3 + x_3 x_2^2 x_1 - x_3^2 x_2} = \frac{h_1}{h_2} - 2,\\
g_4 &= \frac{-x_1 x_2 + x_3 - x_3 x_2^2 x_1 + x_3^2 x_2}{-x_1^2 + 2\,x_3 x_1 - x_3 + x_3 x_2^2 x_1 - x_3^2 x_2} = \frac{h_1}{h_1 - h_2}
\end{aligned}$$

It is clear that it has transcendence degree 2 over $\mathbb{Q}$. *We have*

$$C = \{p_l = g_l(y_1, y_2, y_3) - g_l(x_1, x_2, x_3) : l = 1, \ldots, 4\}.$$

We construct the matrix $A = (a_{i,j})$, *for* $i = 1, \ldots, 3$ *and* $j = 1, \ldots, 4$, *where*

$$a_{i,j} = \frac{\partial p_i}{\partial y_j}(x_1, x_2, x_3).$$

If we put it in triangular form we obtain:

$$\begin{pmatrix} 1 & 0 & -\dfrac{(x_1x_2^2 + x_1^2x_2 - 2\,x_3^2 + x_3x_1 + 2\,x_1 - 1)\,x_1}{x_3x_2x_1^2 + x_1^2 + x_3^2x_1 - x_3 - 2\,x_3^3} \\ 0 & 1 & \dfrac{x_3x_2^2 - x_1 + 2\,x_3}{x_3x_2x_1^2 + x_1^2 + x_3^2x_1 - x_3 - 2\,x_3^3} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

The rank of the matrix is 2 as we expected. On the other hand, x_3 (the generator of the total field corresponding to the last column) is a transcendence basis of $\mathbb{Q}(x_1, x_2, x_3)$ over $\mathbb{Q}(g_1, g_2, g_3, g_4)$.

2.2.1 Jacobian matrix and uni-multivariate decomposition

As an application of the results in this subsection, we will recover the relation between the Jacobian matrix of a polynomial, see Shafarevich (1977), and uni-multivariate decomposition, see Gutierrez, Rubio and Sevilla (2002).

Definition 2 *Given a list of polynomials $\Phi = (p_1, \ldots, p_n)$, where $p_i \in \mathbb{K}[\mathbf{x}]$, we denote by $J(\Phi)$ the Jacobian matrix they define, that is,*

$$J(\Phi) = \begin{pmatrix} \dfrac{\partial p_1}{\partial x_1} & \dfrac{\partial p_1}{\partial x_2} & \cdots & \dfrac{\partial p_1}{\partial x_n} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \dfrac{\partial p_n}{\partial x_1} & \dfrac{\partial p_n}{\partial x_2} & \cdots & \dfrac{\partial p_n}{\partial x_n} \end{pmatrix}$$

Let $r = \text{tr.deg.}(\mathbb{K}(\mathbf{x})/\mathbb{K}(p_1, \ldots, p_n))$. Assume that not every p_i is constant, then $0 \leq r \leq n-1$.

We will prove the following result:

Theorem 6 *These statements are equivalent:*

(i) *There exist $f \in \mathbb{K}[\mathbf{x}]$, $q_i \in \mathbb{K}[t]$ such that $p_i = q_i(f)$, $i = 1, \ldots, n$.*
(ii) *The rank of the matrix $J(\Phi)$ is $n-1$.*

First, we will translate this into a question about fields.

Lemma 1 *The statement (i) in Theorem 6 is equivalent to $r = 1$.*

Proof: If (i) is true, then $\mathbb{K}[p_1, \ldots, p_n] \subset \mathbb{K}[f]$ and $K(p_1, \ldots, p_n) \subset \mathbb{K}(f)$ so tr.deg.$(\mathbb{K}(p_1, \ldots, p_n)/\mathbb{K}) = 1$.

Conversely, if $r = 1$, by the Extended Lüroth's Theorem we have that $\mathbb{K}(p_1, \ldots, p_n) = \mathbb{K}(f)$; as the field contains some non-constant polynomial, by the same theorem we can assume $f \in \mathbb{K}[\mathbf{x}]$. If suffices to prove for each i that $p_i = q_i(f)$, $q_{iD} \in \mathbb{K}^*$.

If $\gcd(q_{iN}, q_{iD}) = 1$, then for some $\alpha_i(t), \beta_i(t) \in \mathbb{K}[t]$ we have

$$1 = q_{iN}(t)\alpha_i(t) + q_{iD}(t)\beta_i(t) \ \Rightarrow\ 1 = q_{iN}(f)\alpha_i(f) + q_{iD}(f)\beta_i(f) \ \Rightarrow$$

$$\Rightarrow\ \gcd(q_{iN}(f), q_{iD}(f)) = 1 \ \Rightarrow\ q_{iD} \in \mathbb{K}^* \ \Rightarrow\ q_i \in \mathbb{K}[t].$$

■

Now consider the ideal of relations of $\mathbb{K}(\mathbf{x})/\mathbb{K}(p_1, \ldots, p_n)$,

$$\mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{K}(p_1,\ldots,p_n)} = \{h(\mathbf{y}) \in \mathbb{K}(p_1, \ldots, p_n)[\mathbf{y}] : \ h(\mathbf{x}) = 0\}$$

where $\mathbf{y} = (y_1, \ldots, y_n)$ and y_i are algebraically independent from x_i. Then we have:

Lemma 2 *Let $\overline{p}_i = p_i(\mathbf{y}) - p_i$. Then*

$$\mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{K}(p_1,\ldots,p_n)} = \langle \overline{p}_1, \ldots, \overline{p}_n \rangle.$$

Proof: "$\supset$" is trivial. Conversely, given $h \in \mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{K}(p_1,\ldots,p_n)}$ we can assume $h \in \mathbb{K}[p_1, \ldots, p_n][\mathbf{y}]$. We write $h = \sum_\alpha h_\alpha(\mathbf{x})\mathbf{y}^\alpha$, where $h_\alpha(\mathbf{x}) \in \mathbb{K}[p_1(\mathbf{x}), \ldots, p_n(\mathbf{x})]$. Then $h(\mathbf{x}, \mathbf{y}) - \sum_\alpha (h_\alpha(\mathbf{x}) - h_\alpha(\mathbf{y}))\mathbf{y}^\alpha = h(\mathbf{y}, \mathbf{y})$. Since $h(\mathbf{x}, \mathbf{x}) = 0$ we also have $h(\mathbf{y}, \mathbf{y}) = 0$. We may write $h_\alpha(\mathbf{x}) = g_\alpha(p_1(\mathbf{x}), \ldots, p_n(\mathbf{x}))$ and do so for $h_\alpha(\mathbf{y})$ to get $g_\alpha(p_1(\mathbf{y}), \ldots, p_n(\mathbf{y}))$. It is then clear that $g_\alpha(p_1(\mathbf{y}), \ldots, p_n(\mathbf{y})) - g_\alpha(p_1(\mathbf{x}), \ldots, p_n(\mathbf{x}))$ belongs the required ideal. ■

Because of Theorem 5, if the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(p_1,\ldots,p_n)$ is separable then

$$\text{rank}\begin{pmatrix} \frac{\partial \overline{p}_1}{\partial y_1}(\mathbf{x}) & \frac{\partial \overline{p}_1}{\partial y_2}(\mathbf{x}) & \ldots & \frac{\partial \overline{p}_1}{\partial y_n}(\mathbf{x}) \\ . & . & \ldots & . \\ . & . & \ldots & . \\ \frac{\partial \overline{p}_n}{\partial y_1}(\mathbf{x}) & \frac{\partial \overline{p}_n}{\partial y_2}(\mathbf{x}) & \ldots & \frac{\partial \overline{p}_n}{\partial y_n}(\mathbf{x}) \end{pmatrix} = n - r.$$

It is clear that the previous matrix is $J(\Phi)$ so the theorem we intend to prove is true if the extension is separable. Besides, we cannot omit the hypothesis of separability, as the next example shows.

Example 3 *Let* $\mathbb{K} = \mathbb{F}_p$, $p = x, q = y^p \in \mathbb{F}_p[x,y]$. *Then*

$$J(p,q) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

but $\text{tr.deg.}(\mathbb{F}_p(x,y^p)/\mathbb{F}_p) = 2$.

Lastly, we have that $p_i = q_i(f)$, $i = 1,\ldots,n$ if and only if $\gcd(\overline{p}_i, \overline{q}_i) \neq 1$ for each i. Also, in this case $\gcd(\overline{p}_i, \overline{q}_i) = \overline{f}$ where $\overline{f} = f(u_1,\ldots,u_n) - f(\mathbf{x})$ and $\mathbb{K}[p_1,\ldots,p_n] = \mathbb{K}[f]$.

3 The case of transcendence degree n

Now we will study the case in which the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(f_1,\ldots,f_m)$ is algebraic.

The problem of computing intermediate subfields in finite algebraic extensions over the rational number field has been studied by several authors, we can mention the paper Landau and Miller (1985) and more recently Klüners and Pohst (1997). Our approach it is a modification and adaptation of Landau and Miller (1985)'s techniques and it is based on some general ideas of Rubio's Ph. D. Thesis, Rubio (2001).

Corollary 1 and Primitive Element Theorem allow us to rewrite the involved fields in the following way:

- There exist rational functions $\hat{\alpha}_1,\ldots,\hat{\alpha}_n$ such that $\mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n)/\mathbb{K}$ is a purely transcendental extension, with

$$\mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n) \subset \mathbb{K}(f_1, \ldots, f_m) \subset \mathbb{K}(x_1, \ldots, x_n).$$

- There exist $\hat{\alpha}_{n+1}, f$ algebraic over $\mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n)$ such that

$$\begin{aligned} \mathbb{K}(f_1, \ldots, f_m) &= \mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n, \hat{\alpha}_{n+1}), \\ \mathbb{K}(x_1, \ldots, x_n) &= \mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n, f). \end{aligned}$$

Also, for any intermediate field in the extension there exists h algebraic over $\mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n)$ such that

$$\mathbb{F} = \mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n, h).$$

The structure of the lattice of intermediate fields in the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(f_1, \ldots, f_m)$ suggests the following diagram: let

$$\begin{array}{rccc} \Phi : & \mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n) & \longrightarrow & \mathbb{E} = \mathbb{K}(t_1, \ldots, t_n) \\ & \hat{\alpha}_i & \longmapsto & t_i \end{array}$$

where $t_1, \ldots, t_n$ are new free variables. Φ is an isomorphism that can be extended to $\mathbb{K}(\mathbf{x})$ by means of an isomorphism $\hat{\Phi}$:

$$\begin{array}{rccc} \hat{\Phi} : & \mathbb{K}(\mathbf{x}) & \longrightarrow & \mathbb{E}[\alpha] \\ & \hat{\alpha}_i & \longmapsto & t_i \\ & f & \longmapsto & \alpha \end{array}$$

We have that $\hat{\Phi}(\mathbb{K}(\mathbf{x}))$ is algebraic over $\mathbb{E}$. By the Primitive Element Theorem, we can write $\hat{\Phi}(\mathbb{K}(\mathbf{x})) = \mathbb{E}[\alpha]$, where α is algebraic over $\mathbb{E}$. $\hat{\Phi}$ is an isomorphism that extends Φ.

On the other hand, f is algebraic over $\mathbb{K}(\hat{\alpha}_1, \ldots, \hat{\alpha}_n)$. Then there exists its minimum polynomial $p_f(\hat{\alpha}_1, \ldots, \hat{\alpha}_n, z)$ and it can be computed with Corollary 1. As $\hat{\Phi}$ is an isomorphism, $p_f(t_1, \ldots, t_n, z)$ is the minimum polynomial of α over $\mathbb{E}$ and $\mathbb{E}[\alpha] = \mathbb{E}[z]/(p_f)$.

Once we have the isomorphism $\hat{\Phi}$, it can be restricted to $\mathbb{K}(f_1, \ldots, f_m)$ or any intermediate field $\mathbb{F}$ of $\mathbb{K}(\mathbf{x})/\mathbb{K}(f_1,\ldots,f_m)$. Analogously we have

$$\begin{array}{rcl} \hat{\Phi}|\mathbb{F}:\ \mathbb{F} & \longrightarrow & \mathbb{E}[\gamma] \\ \hat{\alpha}_i & \longmapsto & t_i \\ h & \longmapsto & \gamma \end{array}$$

where γ is algebraic over $\mathbb{E}$ with minimum polynomial $p_h(t_1,\ldots,t_n,z)$.

Conversely, given a field $\mathbb{E}[\gamma]$ such that $\mathbb{E}[\beta]\subset\mathbb{E}[\gamma]\subset\mathbb{E}[\alpha]$, the inverse of $\hat{\Phi}$ gives the intermediate field $\mathbb{F}=\mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n)(\hat{\Phi}^{-1}(\gamma))$.

The resulting diagram is

Diagram 1

$$\begin{tikzcd}
\mathbb{K}(x_1,\ldots,x_n) \arrow[r, leftrightarrow] & \mathbb{E}[\alpha]=\mathbb{E}[z]/(p_f) \\
\mathbb{F} \arrow[u] \arrow[r, leftrightarrow] & \mathbb{E}[\gamma]=\mathbb{E}[z]/(p_h) \arrow[u] \\
\mathbb{K}(f_1,\ldots,f_m) \arrow[u] \arrow[r, leftrightarrow] & \mathbb{E}[\beta]=\mathbb{E}[z]/(p_{\hat{\alpha}_{n+1}}) \arrow[u] \\
\mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n) \arrow[u] \arrow[r, leftrightarrow] & \mathbb{E} \arrow[u]
\end{tikzcd}$$

This diagram is interesting because we can decide computationally the inclusion of these fields.

Theorem 7 *Let $\mathbb{E}[\alpha]/\mathbb{E}$ be an algebraic extension and $\mathbb{E}[\beta],\mathbb{E}[\gamma]\subset\mathbb{E}[\alpha]$ intermediate fields. Then we can decide if $\mathbb{E}[\beta]\subset\mathbb{E}[\gamma]$.*

Proof: A subfield $\mathbb{E}[\beta]$ of $\mathbb{E}[\alpha]$ is determined by means of the minimum polynomial of β over $\mathbb{E}$, p_β, and by a polynomial $f\in\mathbb{E}[x]$ such that $\beta=f(\alpha)$. If $\mathbb{E}[\beta]\subset\mathbb{E}[\gamma]$, then $\beta=p(\gamma)$ where $\deg\ p<\deg\ p_\gamma$, that is, $\beta=a_{l-1}\gamma^{l-1}+\cdots+a_0$. On the other hand, $\beta,\gamma\in\mathbb{E}[\alpha]$, so deciding if $\mathbb{E}[\beta]\subset\mathbb{E}[\gamma]$ can be done by solving a system of linear equations with $\deg\ p_\alpha$ equations (as $\{1,\alpha,\ldots,\alpha^{\deg\ p_\alpha-1}\}$ is a basis of the $\mathbb{E}$-vector space $\mathbb{E}[\alpha]$), and $\deg\ p_\gamma$ variables $a_{l-1},\ldots,a_0$. ■

In (Lazard and Valibouze, 1993) there is another method to decide field inclusion using resolvents when $\mathbb{E}=\mathbb{Q}$.

As a consequence we have that the problem is solved for fields with characteristic zero if we can find all intermediate fields of the algebraic extension $\mathbb{E}[\alpha]/\mathbb{E}$. Now we will study how to find those fields.

We will denote by $\mathbb{L} = \mathbb{E}[\alpha_1, \ldots, \alpha_m]$ the splitting field of $\mathbb{E}[\alpha]$, being $\alpha = \alpha_1$. Due to Galois Theory we know that there is a bijection between the lattice of intermediate fields of $\mathbb{E} \subset \mathbb{L}$ and the subgroups of the Galois group of $\mathbb{E} \subset \mathbb{L}$, which we will denote as G. If we define $G_\alpha = \{\sigma \in G : \ \sigma(\alpha) = \alpha\}$, there is also a bijection between the subgroups of $G_\alpha \subset G$ and certain roots of the minimum polynomial p_α of α. These correspondences are the key to the method that we present to find intermediate fields of simple algebraic extensions. First, we present an adapted version of the classical fundamental theorem of Galois theory.

Theorem 8 *There exists a bijection between the set of intermediate fields of $\mathbb{E} \subset \mathbb{E}[\alpha]$ and the set of subgroups of G that contain G_α.*

So, we can work with the Galois group of the extension, for which we will use the so called decomposition blocks, that we introduce now, see (Wielandt, 1964).

Definition 3 *Let $f \in \mathbb{K}[x]$ be an irreducible polynomial, G the Galois group of f over $\mathbb{K}$ and $\Omega = \{\alpha = \alpha_1, \ldots, \alpha_m\}$ the set of roots of f.*

A subset $\psi \subset \Omega$ is a decomposition block *if for each $\sigma \in G$ we have either $\sigma(\psi) \cap \psi = \emptyset$ or $\sigma(\psi) = \psi$.*

The blocks $\{\alpha_i\}$ and Ω are called trivial blocks.

The set of blocks that are conjugate to ψ, that is $\psi, \sigma_2(\psi), \ldots, \sigma_r(\psi)$, are a block system.

*If $|\psi| = s$ we say that the block ψ is a $r \times s$-*decomposition block, *where $(m = rs)$.*

The next theorem gives a bijection between the intermediate groups of $G_\alpha \subset G$ and the decomposition blocks that contain α. The proof is an adaptation of the one in (Wielandt, 1964).

Theorem 9 *There exists a bijection between the set of intermediate groups of $G_\alpha \subset G$ and the set of decomposition blocks that contain α. Besides, the correspondence respects inclusions.*

Proof: We define the following bijection:

$$\begin{array}{ccc} \{H:\ G_\alpha \subset H \subset G\} & \longrightarrow & \{\psi:\ \alpha \in \psi\} \\ H & \longmapsto & \psi_H = \{\sigma(\alpha):\ \sigma \in H\} \end{array}$$

In order to see that it is well defined we must prove that ψ_H is a decomposition block. Let $\sigma \in G$ and assume that $\beta \in \sigma(\psi_H) \cap \psi_H$. By definition there exist $\tau_1, \tau_2 \in H$ such that $\beta = \tau_1(\alpha) = \sigma(\tau_2(\alpha))$, this implies that $\tau_1^{-1}\sigma\tau_2 \in G_\alpha \subset H$. In this way we have that $\sigma \in H$ and thus $\sigma(\psi_H) = \psi_H$. Also, $\alpha \in \psi_H$.

Now let H_1, H_2 be subgroups of $G_\alpha \subset G$ such that $\psi_{H_1} = \psi_{H_2}$. If $\sigma \in H_1$, there exists $\tau \in H_2$ with $\sigma(\alpha) = \tau(\alpha)$. Then $\tau^{-1}\sigma \in G_\alpha \subset H_2$ and so $\sigma \in H_2$.

Let ψ be a decomposition block with $\alpha \in \psi$. The inverse image of ψ is the subgroup $H = \{\sigma \in G :\ \sigma(\psi) = \psi\}$. Indeed, H is a subgroup and $G_\alpha \subset H$. We will see that $\psi = \psi_H$:

Let $\beta \in \psi$. As G is transitive there exists $\sigma \in G$ such that $\beta = \sigma(\alpha)$. On the other hand, $\alpha, \beta \in \psi$, so $\sigma \in H$ and $\beta \in \psi_H$. Conversely, if $\beta \in \psi_H$, there exists $\sigma \in H$ such that $\beta = \sigma(\alpha)$, and as $\sigma(\psi) = \psi$ we have $\beta \in \psi$.

It is trivial that this bijection respects inclusions. ■

The correspondences described so far allow us to construct the following diagram:

$$\begin{tikzcd}
\mathbb{L} \arrow[r, leftrightarrow] & \{id\} \arrow[d] & \\
\mathbb{E}[\alpha] \arrow[u] \arrow[r, leftrightarrow] & G_\alpha \arrow[r, leftrightarrow] \arrow[d] & \{\alpha\} \arrow[d] \\
\mathbb{F} \arrow[u] \arrow[r, leftrightarrow] & H \arrow[r, leftrightarrow] \arrow[d] & \{\alpha_{i_1}, \ldots, \alpha_{i_j}\} \arrow[d] \\
\mathbb{E} \arrow[u] \arrow[r, leftrightarrow] & G \arrow[r, leftrightarrow] & \{\alpha_1, \ldots, \alpha_m\}
\end{tikzcd}$$

It is important to highlight that, given a decomposition block ψ, we can directly compute the corresponding field $\mathbb{F}_\psi$ without computing the corresponding group.

Theorem 10 *Let $\psi = \{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$ be a decomposition block, then the corresponding field in the previous diagram is $\mathbb{E}[\beta_1, \ldots, \beta_k]$ where each β_j is the*

j-th elementary symmetric function in $\alpha_{i_1}, \dots, \alpha_{i_k}$.

Proof: Let $h(z) = \prod_{j=1}^{k}(z - \alpha_{i_j}) = z^k + a_{k-1}z^{k-1} + \cdots + a_0$, then

$$\mathbb{E}[\beta_1, \dots, \beta_k] = \mathbb{E}[a_{k-1}, \dots, a_0].$$

We will see that $\mathbb{E}[a_{k-1}, \dots, a_0] = \mathbb{E}_\psi$:

Let $\sigma \in G_\psi$, then $\sigma(h) = h$ and $\sigma(a_i) = a_i$ for every i. That is, $\mathbb{E}[a_{k-1}, \dots, a_0] \subset \mathbb{E}_\psi$.

Now let $\sigma \in G_{\mathbb{E}[a_{r-1},\dots,a_0]}$, then $\sigma(a_i) = a_i$ for each i. Therefore $\sigma(h) = h$ and $\sigma(\psi) = \psi$, and $\mathbb{E}_\psi \subset \mathbb{E}[a_{k-1}, \dots, a_0]$. ■

Next, we will show the results that will support the algorithm that solves our problem.

Lemma 3 *Let $q(z, \alpha)$ be an irreducible factor of p_α, the minimum polynomial of α, and ψ a decomposition block that contains α. If a root of $q(z, \alpha)$ is in ψ, then all the roots of $q(z, \alpha)$ are in ψ.*

Depending on the factorization of the minimum polynomial we have different methods to compute the decomposition blocks. We will assume that

$$p_\alpha(z) = (z - \alpha)p_2(z, \alpha) \cdots p_l(z, \alpha).$$

Among the next results, the first one is interesting in itself, because we can easily compute the intermediate fields when the extension is normal.

Theorem 11 *If $\mathbb{E}[\alpha]/\mathbb{E}$ is normal, we can compute all the intermediate fields; and one of them on polynomial time if the algebraic degree of the extension is not prime.*

Proof: Assume that $p_\alpha(z) = (z-\alpha)(z-p_2(\alpha)) \cdots (z-p_l(\alpha))$. Then the Galois group of p_α over $\mathbb{E}$ is $G = \{\sigma_i : \alpha \mapsto p_i(\alpha),\ i = 1, \dots, l\}$. Each subgroup H of G corresponds with a subfield $\mathbb{F} = \mathbb{E}[a_0, \dots, a_{l-1}]$ with $x^l + a_{l-1}x^{l-1} + \cdots + a_0 = \prod\limits_{\sigma \in H}(z - \sigma(\alpha))$.

Also, a group G has non-trivial subgroups if and only if $|G| = l = [\mathbb{E}[\alpha] : \mathbb{E}]$ is composite. ■

Theorem 12 *If the extension $\mathbb{E}[\alpha]/\mathbb{E}$ is not normal and p_α has more than one root in $\mathbb{E}[\alpha]$, there exists a field $\mathbb{F}$ such that $\mathbb{E} \subsetneq \mathbb{F} \subsetneq \mathbb{E}[\alpha]$.*

Proof: If

$$p_\alpha(z) = (z-\alpha)(z-p_2(\alpha))\cdots(z-p_{l'}(\alpha))\cdot p_{l'+1}(z,\alpha)\cdots p_l(z,\alpha)$$

is the complete factorization of p_α, then $H = \{\sigma_i : \alpha \mapsto p_i(\alpha),\ i = 1,\ldots,l'\}$ is a subgroup of G. Indeed, let $\sigma_i, \sigma_j \in H$, then

$$\begin{aligned} p_\alpha(z) &= \sigma_j(p_\alpha(z)) \\ &= \sigma_j((z-\alpha)(z-p_2(\alpha))\cdots(z-p_{l'}(\alpha))p_{l'+1}(z,\alpha)\cdots p_l(z,\alpha)) \\ &= (z-p_j(\alpha))(z-p_2(p_j(\alpha)))\cdots(z-p_{l'}(p_j(\alpha)))\cdots \\ &\quad \cdots p_{l'+1}(z,p_j(\alpha))\cdots p_l(z,p_j(\alpha)) \end{aligned}$$

is another factorization of p_α in $\mathbb{E}[\alpha]$. Then there exists $k \in \{1,\ldots,l'\}$ such that $\sigma_i\sigma_j(\alpha) = p_i(p_j(\alpha)) = p_k(\alpha) = \sigma_k(\alpha)$. Therefore, $\langle H \cup G_\alpha\rangle$ is a subgroup of $G_\alpha \subset G$; and it is non-trivial since G is transitive over the roots of p_α and $\langle H \cup G_\alpha\rangle$ is not.

Because of this, $\mathbb{E}[a_0,\ldots,a_{l'-1}]$ is an intermediate field of $\mathbb{E} \subset \mathbb{E}[\alpha]$, being

$$x^{l'} + a_{l'-1}x^{l'-1} + \cdots + a_0 = \prod_{i=1}^{l'}(z - p_i(\alpha)).$$

■

The remaining case is that in which p_α has exactly one linear factor. In this case, one must combine the factors of p_α to check which of those divisors provide an intermediate field. In the worst case, we must check an exponential number of factors; but in other cases, we can find subfields even if we don't have the complete factorization of p_α.

As it is made clear before, we need to factorize polynomials whose coefficients are in some algebraic extension of the field we work in. Next, we will give the details of a method to compute such a factorization. We will show that the algorithm in (Trager, 1976) that factors polynomials is in random polynomial time if the base field is a rational function field over $\mathbb{K}$ and there is a polynomial time algorithm to factorize univariate polynomials over $\mathbb{K}$.

We will adapt the algorithm to fields $\mathbb{E}$, $\mathbb{F}$ where $\mathbb{F}/\mathbb{E}$ is a finite algebraic separable extension. We will also present some slightly shorter proofs of some results. The idea is similar to the one presented in (van der Waerden, 1964), but more efficient from the computational point of view. It is based on the fact that the polynomial $f(x - c\alpha) \in \mathbb{E}[\alpha]$ and its norm have essentially the same factorization unless the norm is not square free. Trager's reduction is used in (Landau, 1985) to provide an algorithm in polynomial time to factorize polynomials in algebraic number fields, using the known univariate factorization algorithm over the rationals in (Lenstra, Lenstra and Lovász, 1982).

The situation we are interested in is given by a field extension

$$\mathbb{E} \subset \mathbb{E}(\alpha_1, \ldots, \alpha_m) = \mathbb{F}$$

that is algebraic and separable. This satisfies the hypothesis of the Primitive Element Theorem; a constructive version for the case $\mathbb{E} = \mathbb{Q}$ is in (Yokoyama, Noro and Takeshima, 1989). The proof for an arbitrary algebraic extension is similar. Other methods can be found in (Loos, 1983).

In the following we will use these notations:

Notation 1

- $\mathbb{F}/\mathbb{E}$ *is a finite separable algebraic extension.*
- *Due to the Primitive Element Theorem we can write* $\mathbb{F} = \mathbb{E}[\alpha]$.
- p_α *is the minimum polynomial of* α *over* $\mathbb{E}$.
- $\alpha_1, \ldots, \alpha_l$ *are the roots of* p_α *in* $\overline{\mathbb{E}}$, *the algebraic closure of* $\mathbb{E}$.
- G *is the Galois group of* p_α *over* $\mathbb{E}$.

Let us remember the definition of the norm of a polynomial:

Definition 4 *Let* $f(\alpha, x) \in \mathbb{F}[x]$. *We define the* norm *of* f *as*

$$\mathrm{N}(f) = \prod_{i=1}^{l} f(\alpha_i, x).$$

Using the known properties of the resultant, we have

$$\mathrm{N}(f) = \mathrm{Res}_t(p_\alpha(t), f(t, x)) \in \mathbb{E}[x].$$

The following is a classical result about the norm.

Proposition 3 *Let* $f(\alpha, x) \in \mathbb{F}[x]$ *be an irreducible polynomial. Then* $\mathrm{N}(f)$ *is a power of an irreducible polynomial over* $\mathbb{E}$.

The key result in (Trager, 1976) is the following:

Theorem 13 *Let* $f(\alpha, x) \in \mathbb{F}[x]$ *be an irreducible polynomial such that* $\mathrm{N}(f)$

is square free. If $\mathrm{N}(f) = h_1 \cdots h_m$ *is a complete factorization in* $\mathbb{E}[x]$*, then*

$$f = \gcd(h_1, f) \cdots \gcd(h_m, f)$$

is a complete factorization of f *in* $\mathbb{F}[x]$*.*

With the results we have presented, we can factorize a polynomial over $\mathbb{F}$ if $\mathbb{E}$ has an algorithm for univariate factorization, except when the norm of the polynomial is not square free. To avoid this we can apply a map $x \mapsto x - c\alpha$. Such a map always exists because of a simple result due to Kronecker.

Theorem 14 (Kronecker) *Let* $f(\alpha, x) \in \mathbb{F}[x]$ *be a square free polynomial with degree* m*. Assume that* $l = [\mathbb{F} : \mathbb{E}]$ *and* $\mathbb{E}$ *has more than* $\dfrac{l(l-1)m(m-1)}{2}$ *non-zero elements. Then there exists* $c \in \mathbb{E}$ *such that* $\mathrm{N}(f(\alpha, x - c\alpha))$ *is square free.*

The combination of these results provides the following factorization algorithm.

Algorithm 1

```
INPUT: $f(\alpha, x) \in \mathbb{E}[\alpha][x]$.
OUTPUT: a complete factorization $f_1(\alpha, x), \ldots, f_m(\alpha, x)$ of $f(\alpha, x)$ in $\mathbb{E}[\alpha][x]$.

A. Find $c \in \mathbb{E}$ such that $\mathrm{N}(f(\alpha, x - c\alpha))$ is square free.
B. Factor $\mathrm{N}(f(\alpha, x - c\alpha))$ in $\mathbb{E}[x]$ to obtain a complete factorization

      $\mathrm{N}(f(\alpha, x - c\alpha)) = h_1 \cdots h_m$.

C. Compute $f_i = \gcd(f, h_i(x + c\alpha))$. Return the $f_i$'s.
```

Analysis: We will analyze the algorithm in our particular setting. We are interested in $\mathbb{E}$ being a rational function field $\mathbb{E} = \mathbb{K}(\mathbf{x})$ over $\mathbb{K}$. Factorization over $\mathbb{K}(\mathbf{x})[x]$ is equivalent to factorization in the ring of polynomials $\mathbb{K}[x_1, \ldots, x_n, x]$. On the other hand it is known that every factorization algorithm in polynomial time in $\mathbb{K}[x]$ provides one in random polynomial time in $\mathbb{K}[x_1, \ldots, x_n][x]$, using Hilbert's Irreducibility Theorem, see (von zur Gathen and Gerhard, 1999) and (Zippel, 1993).

Also, if the number of variables is zero ($n = 0$), the previous result by Kronecker requires that the field $\mathbb{K}$ has at least l^2m^2 elements, where m is the degree of the polynomial and $l = [\mathbb{F} : \mathbb{E}]$. If $n > 0$ there is always an adequate $\alpha \in \mathbb{E}[x]$, as $\mathbb{E}$ is infinite.

Finally, step C requires the computation of several gcd's in $\mathbb{E}[\alpha]$. This is also in polynomial time due to Euclides' Algorithm, for more details of this part see (Landau and Miller, 1985) for $\mathbb{Q}$. ■

Summarizing the results we have presented in this section, we have the following algorithm to find intermediate unirational fields over a given field, if the extension is separable and algebraic.

With the above notation:

Algorithm 2

```
INPUT: An irreducible $f(t) \in \mathbb{E}[t]$, such that $f(\alpha) = 0$ and $p_\alpha(z) \in E[\alpha][z]$.
OUTPUT: All $h(t) \in \mathbb{E}[t]$ such that $\mathbb{E}[h(\alpha)] \subset \mathbb{E}[\alpha]$.

A. Factorize $p_\alpha(z)$ in $E[\alpha]$.
B.1. If $p_\alpha(z)$ has more than one linear factor:
        $p_\alpha(z) = (z-\alpha)(z-p_2(\alpha))\cdots(z-p_r(\alpha))p_{r+1}(z,\alpha)\cdots p_{r'}(z,\alpha).$
    — Compute a minimal subgroup $G_\psi$ of $\langle\{\sigma_2 : \alpha \mapsto p_i(\alpha)\}\rangle$.
    — Consider $h(z) = \prod_{\sigma \in G_\psi}(z - \sigma(\alpha)) = a_u x^u + \cdots + a_0$.
    — Take $a_i$ such that $\mathbb{E}[a_i]$ is a proper subfield of $\mathbb{E} \subset \mathbb{E}[\alpha]$.
B.2. If $p_\alpha(z) = (z-\alpha)p_2(z,\alpha)\cdots p_{r'}(z,\alpha)$, with $p_i$ non-linear:
    — Consider a factor $P_2(z) = h(z,\alpha)(z-\alpha)$ of $p_\alpha(z)$,
            $P_2 = (z-\alpha)h(z,\alpha) = a_u x^u + \cdots + a_0.$
    — If $\mathbb{E}[a_i] = \mathbb{E}[\alpha]$ for all $i$, then take another factor.
```

We illustrate this algorithm with the following example:

Example 4 *Consider the rational functions f_1, f_2 in $\mathbb{Q}(x,y)$ in Example 1*

$$f_1 = -y^2x - y^4 + 2\,x + 2\,y^2 - 1,\ \ f_2 = 4\,y^4 - 10\,y^2 + 5 + 3\,y^2x - 6\,x.$$

Our goal is computing all intermediate fields in the extension $\mathbb{Q}(x,y)/\mathbb{Q}(f_1,f_2)$.

By Example 1, we know it is an algebraic extension of degree 4. Moreover, y is a primitive element and its minimum polynomial is

$$p_y(f_1,f_2,z) = z^4 + z^2 - 3f_1 - f_2 + 2.$$

Clearly, if α is a root of $p_y(t_1,t_2,z)$, then also $-\alpha$ is a root, so we have a factorization

$$p_y(t_1,t_2,z) = (z-\alpha)(z+\alpha)(z^2+\alpha^2-4)$$

in $E[\alpha] = E[z]/(p_y)$.

Let $H = \{id, \alpha \to -\alpha\}$ and $h(z) = z^2 - \alpha^2$, we obtain the proper field $\mathbb{E} \subset \mathbb{E}[\alpha^2] \subset \mathbb{E}[\alpha]$

$$\mathbb{Q}(f_1, f_2) \subsetneq \mathbb{Q}(f_1, f_2, y^2).$$

To determine all intermediate fields, we need to factorize $p_y(t_1, t_2, z) = (z - \alpha)(z + \alpha)(z^2 + \alpha^2 - 4)$. In order to do this we will use Algorithm 1. As the polynomial $g(z, \alpha) = z^2 + \alpha^2 - 4$ divides the polynomial $p_y(t_1, t_2, z)$, we apply a transformation (see Theorem 14), for example $z \to z - 3\alpha$. The next step is computing the norm of $g(z - 3, \alpha)$.

$$\begin{aligned} N(g(z - 3\alpha, \alpha)) &= \mathrm{Res}_z(p_y(t_1, t_2, z), (z - 3\alpha)^2 + \alpha^2 - 4) \\ &= 4 - 4\, t_{\mathit{2}} + 6\, t_{\mathit{1}}\, t_{\mathit{2}} + {t_{\mathit{2}}}^2 - 12\, t_{\mathit{1}} - 1568\, \alpha^2 + 10784\, \alpha^4 \\ &\quad +9\, {t_{\mathit{1}}}^2 - 1104\, t\mathit{1}\, \alpha^2 - 816\, t_1\, \alpha^4 - 368\, t_{\mathit{2}}\, \alpha^2 \\ &\quad -272\, t_{\mathit{2}}\, \alpha^4 - 13312\, \alpha^6 + 4096\, \alpha^8. \end{aligned}$$

As $N(g(z - 3\alpha, \alpha))$ is irreducible, also $z^2 + \alpha^2 - 4$ is and we already have a complete factorization of the minimum polynomial. Therefore, the extension is not normal and in order to find more intermediate fields we only have to consider the divisor $(z - \alpha)(z^2 + \alpha^2 - 4)$; but it cannot provide a decomposition block, as 3 does not divide the degree of the extension.

The lattice of fields is then

$$\mathbb{Q}(f_1, f_2) \subsetneq \mathbb{Q}(f_1, f_2, y^2) \subsetneq \mathbb{Q}(x, y).$$

Finally, we note that the intermediate field we found is rational, in fact

$$\mathbb{Q}(f_1, f_2, y^2) = \mathbb{Q}(x - y, x + y^2) = \mathbb{Q}(x, y^2).$$

However, as we said, our algorithm always returns a number of generators which is equal to the transcendence degree plus one (see Theorem 2).

3.1 Normality and monodromy group

The computation of intermediate fields is even more interesting and simpler when the algebraic extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(f_1, \ldots, f_m)$ is normal. In this case we have the known bijection between subgroups of the Galois group and intermediate fields. We will now concentrate on the case $n = 1$ and assume that char $\mathbb{K} = 0$. Our problem can be stated in the following way:

Problem 3 *Given an irreducible polynomial $f \in \mathbb{K}[x]$, determine if the extension $\mathbb{K}(\alpha)/\mathbb{K}$, where $\mathbb{K}(\alpha) = \mathbb{K}[x]/(f)$, is normal.*

We can use simple Galois techniques to decide this matter. Remember that we assume that the extension $\mathbb{K}(x)/\mathbb{K}(f)$ is algebraic.

Definition 5 *Let $f \in \mathbb{K}(x)$. We define the* monodromy group *of f to be the Galois group of the extension $\mathbb{K}(x)/\mathbb{K}(f)$. That is, if we denote by $\mathbb{F}$ the splitting field of the extension $\mathbb{K}(x)/\mathbb{K}(f)$, then the monodromy group of f is the group of automorphisms of $\mathbb{F}$ that leave $\mathbb{K}(f)$ fixed.*

Theorem 15 *The extension $\mathbb{K}(x)/\mathbb{K}(f)$ is normal if and only if $G(f) = \{u \in \mathrm{Aut}_{\mathbb{K}} \mathbb{K}(x) : f \circ u = f\}$ is equal to the monodromy group of the extension.*

Proof: the roots of the minimum polynomial are the images of one of them through the elements of the Galois group; if it is equal to $G(f)$, they are all in $\mathbb{K}(f)$. ■

Corollary 3 *The extension $\mathbb{K}(x)/\mathbb{K}(f)$ is normal if and only if $|G(f)| = \deg\ f$.*

Also, the techniques for factorization in algebraic extensions that we discussed above provide another method: we factorize the polynomial f in $\mathbb{K}(\alpha)$, then the extension is normal if and only if f splits in this field.

Remark 1 *If the extension is normal, factorization in extensions is actually performed over the base field, which greatly improves the efficiency of the algorithm.*

Finally, we can also try to decide normality simply by writing the corresponding equations. In particular, the extension is normal if and only if all the roots of f are in $\mathbb{K}(\alpha)$. There is a known bijection between the polynomials $p(x) \in \mathbb{K}[x]$ with $\deg\ p \leq \deg\ f$ and the elements of $\mathbb{K}(\alpha)$, namely the morphism $x \to \alpha$ from $\mathbb{K}[x]$ to $\mathbb{K}(\alpha)$; therefore, each p represents a root of f in $\mathbb{K}(\alpha)$ if and only if $f(p) = 0$ in $\mathbb{K}(\alpha)$, that is , $f(x)$ divides $f(p(x))$ in $\mathbb{K}[x]$. This is precisely the classic problem of ideal decomposition, see (Casperson, Ford and McKay, 1996).

The previous relation can be expressed directly with equations: let

$$
\begin{aligned}
f &= x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\\
p &= b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,\\
q &= x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0, \quad m = n(n-2).
\end{aligned}
$$

Then from the expression $f(p) = f \cdot q$ we obtain a linear system of equations in the variables b_i and c_j. Note that we are only interested in the existence and computation of values for the variables b_i.

As indicated in the introduction, the particular case in which the given field has transcendence degree one over $\mathbb{K}$ was solved in (Gutierrez, Rubio and Sevilla, 2001).

4 The general case and its reduction to the algebraic case

Our strategy for the resolution of the general problem comes down to reducing it to the case where the given field has transcendence degree n over $\mathbb{K}$, that is, the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(f_1, \ldots, f_m)$ is algebraic. To that end we will present two different methods, and also the outline of another one.

4.1 Relative algebraic closure

We will look for the minimum field that contains all the intermediate algebraic fields over the given one. To this end we adapt the method in (Brennan and Vasconcelos, 1993) and in the recent book (Vasconcelos, 1998) to compute the closure of a ring monomorphism.

Definition 6 *Let $R_1 \subset R_2$ be a ring extension. We call* integral closure of R_1 relative to R_2 *to the subring of R_2 formed by the elements that are integral over R_1.*

In our case, we need to compute the algebraic closure $\mathbb{F}_0$ of the field extension $\mathbb{K}(f_1, \ldots, f_m) \subset \mathbb{K}(\mathbf{x})$. Our goal is to determine explicitly a finite set of generators of the field $\mathbb{F}_0$, in particular as many as the transcendence degree plus one. The Theorem 2 proves that such a set exists.

There are several methods to compute the integral closure of an integral domain in its field of fractions, see for example (Seidenberg, 1975) and the more recent (Gianni and Trager, 1997). The idea in (Brennan and Vasconcelos, 1993) is to compute the integral closure of a birational morphism:

Theorem 16 *Let $\mathbb{D}_1 \subset \mathbb{D}_2$ be an extension of integral domains that are finitely generated over a computable field $\mathbb{K}$ with the same field of fractions (that is, a* birational morphism*). Let $\overline{\mathbb{D}}_1$ be the integral closure of $\mathbb{D}_1$ in its field of fractions. Assume that $\mathbb{D}_2$ is generated over $\mathbb{D}_1$ by fractions whose denominators are powers of some element d. Let r be such that $\overline{\mathbb{D}}_1 d^{r+1} \cap \mathbb{D}_1 \subset (d)$. Then the integral closure of $\mathbb{D}_1$ in $\mathbb{D}_2$ is*

$$d^{-r}(d^r\mathbb{D}_2 \cap d^r\overline{\mathbb{D}}_1 \cap \mathbb{D}_1).$$

We are in the most general situation, that is, $\mathbb{D}_1 \subset \mathbb{D}_2$ is an extension of integral domains that are finitely generated over a computable field $\mathbb{K}$. We will follow these steps,see (Vasconcelos, 1998):

1. We write $\mathbb{D}_2 = \mathbb{D}_1[b_1, \ldots, d_r]$.
2. Let t be a new variable and $\mathbb{D} = \mathbb{D}_1[t, b_1, \ldots, d_r] \subset \mathbb{D}_2[t]$. It is a birational monomorphism.
3. We compute the integral closure $\overline{\mathbb{D}}$ of the extension $\mathbb{D} \subset \mathbb{D}_2[t]$ according to the previous theorem.
4. Then the integral closure of the extension $\mathbb{D}_1 \subset \mathbb{D}_2$ is

$$\overline{\mathbb{D}} \cap \mathbb{D}_2.$$

First we reduce the problem to integral closures of the corresponding integral domains:

Theorem 17 *Let $\mathbb{D}_1 \subset \mathbb{D}_2$ be two integral domains. Let $\mathbb{D}$ be the integral closure of $\mathbb{D}_1$ with respect to $\mathbb{D}_2$. Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be the fields of fractions of $\mathbb{D}_1$ and $\mathbb{D}_2$ respectively and $\mathbb{K}$ the algebraic closure of $\mathbb{K}_1$ with respect to $\mathbb{K}_2$. Then $\mathbb{K}$ is the field of fractions of $\mathbb{D}$.*

Proof: Let $S = \mathbb{D}_1^*$ be the closed multiplicative system of non-zero elements in the integral domain $\mathbb{D}_1$. Then $S^{-1}\mathbb{D}$ is, see (Atiyah and MacDonald, 1969), the integral closure of

$$S^{-1}\mathbb{D}_1 \subset S^{-1}\mathbb{D}_2.$$

As $\mathbb{K}_1 = S^{-1}\mathbb{D}_1 \subset S^{-1}\mathbb{D}$ is integral and $S^{-1}\mathbb{D}_1$ is a field, then $S^{-1}\mathbb{D}$ is a field. Indeed, let α be an integral element over $\mathbb{K}_1$; dividing the equation by a power of α, we can write α^{-1} as an element of $S^{-1}\mathbb{D}$. Finally, in the same way we prove that $S^{-1}\mathbb{D}_2$ is a field, so it is equal to the field of fractions $\mathbb{K}_2$ of the domain $\mathbb{D}_2$. ■

The next step is to rewrite our data according to (Vasconcelos, 1998):

- Let f be the minimum common denominator of the rational functions $f_i \in \mathbb{K}(\mathbf{x})$.
- Let $\Phi : \mathbb{K}[y_1, \dots, y_m] \to \mathbb{K}[\mathbf{x}, 1/f]$, defined as $\Phi(y_i) = f_i$ for each $i = 1, \dots, m$.
- Let $\mathbb{D}_1 = \Phi(\mathbb{K}[y_1, \dots, y_m]) = \mathbb{K}[f_1, \dots, f_m]$. We have that $\mathbb{D}_1 = \mathbb{K}[y_1, ..., y_m]/\mathrm{Ker}(\Phi)$ is a finitely generated $\mathbb{K}$-algebra. Also, the field of fractions of $\mathbb{D}_1$ is $\mathbb{K}(f_1, ..., f_m)$.
- Let $\mathbb{D}_2 = \mathbb{D}_1[\mathbf{x}] = \mathbb{K}[\mathbf{x}, 1/f]$. The field of fractions of $\mathbb{D}_2$ is $\mathbb{K}(\mathbf{x})$.

4.2 Algorithm for the general case

Summarizing the results we have presented, we have the following algorithm to find intermediate unirational fields over a given field, if the extension is separable.

Algorithm 3

INPUT*:* $f_1, \dots, f_m \in \mathbb{K}(\mathbf{x})$.
OUTPUT*: rational functions* $h_1, \dots, h_r$ *such that*

$$\mathbb{K}(f_1, \dots, f_m) \subsetneq \mathbb{K}(h_1, \dots, h_r) \subsetneq \mathbb{K}(\mathbf{x}).$$

A. *Compute the algebraic closure of* $\mathbb{K}(f_1, \dots, f_m)$ *relative to* $\mathbb{K}(\mathbf{x})$ *according to Subsection 4.1.*
B. *Find a separating basis of* $\mathbb{K}(f_1, \dots, f_m)$ *according to Subsection 2.2.*
C. *Rewrite the fields according to Diagram 1.*
D. *Factor the minimum polynomial obtained in the algebraic extension.*
E. *Compute the decomposition blocks that correspond to the factors found before.*
F. *If such a block exists, due to Theorem 10, we compute an intermediate field.*
G. *Recover the generators of the intermediate field in terms of the variables* $x_1, \dots, x_n$.

The following simple example follows the previous algorithm, but also shows a new way in which intermediate fields can be computed more efficiently in some cases.

Example 5 *Let* $\mathbb{F} = \mathbb{Q}(x^4, y^6) \subset \mathbb{Q}(x, y, z)$*. We want to find intermediate fields of transcendence degree 2.*

First, we will prove that the algebraic closure of $\mathbb{F}$ *in* $\mathbb{Q}(x, y, z)$ *is* $\mathbb{Q}(x, y)$*. Indeed, it is clear that this field is algebraic over* $\mathbb{F}$*; on the other hand, no* *element $f \in \mathbb{Q}(x,y,z)$ with $\deg_z f > 0$ can be algebraic over $\mathbb{F}$, as we would have a non-zero polynomial that involves x, y, z.*

As the closure of $\mathbb{F}$ in $\mathbb{Q}(x,y,z)$ is a rational field, we can easily find intermediate fields: we decompose the generators and obtain $1, x^2, x^4, y^2, y^3, y^6$. Each of the fields $\mathbb{Q}(x^4, y^6, f)$ where f is one of the previous functions, is an intermediate algebraic field. Not all of them can be expressed in this way, for example $\mathbb{Q}(x^4, y^6, x+y)$. But we can construct linear combinations of those to find primitive elements, in the same way as in Theorem. As there are finitely many fields, this method may be a way of computing them efficiently.

4.3 Dimension and transcendence degree

Now we present another method that reduces the general case to the algebraic case. This time we will make use of the following theorem, see (Nagata, 1993) and (Alonso, Gutierrez and Rubio, 1999).

Theorem 18 *Let $x_1, \dots, x_n$ be algebraically independent over an infinite field $\mathbb{K}$. If $\mathbb{F}$ is a unirational field with $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(x_1, \dots, x_n)$, there exist $y_1, \dots, y_d$ algebraically independent over $\mathbb{K}$ such that $\mathbb{F} \subset \mathbb{K}(y_1, \dots, y_d)$, where $d =$ tr.deg.$(\mathbb{K}/\mathbb{F})$.*

The following algorithm is based on the proof given in the cited paper.

Algorithm 4

```
INPUT: $f_1, \dots, f_m \in \mathbb{K}(\mathbf{x})$.
OUTPUT: an injective homomorphism $\Phi : \mathbb{K}(f_1, \dots, f_m) \rightarrow \mathbb{K}(x_{i_1}, \dots, x_{i_d})$
  where $d =$ tr.deg.$(\mathbb{K}(f_1, \dots, f_m)/\mathbb{K})$.

A. Compute functions $\overline{f}_1, \dots, \overline{f}_m$ such that:
    — $\mathbb{K}(\overline{f}_1, \dots, \overline{f}_m) = \mathbb{K}(f_1, \dots, f_m)$.
    — $\overline{f}_1, \dots, \overline{f}_d$ are algebraically independent over $\mathbb{K}$.
    — $\overline{f}_{d+1}, \dots, \overline{f}_m$ are integral over $\mathbb{K}[\overline{f}_1, \dots, \overline{f}_d]$.
  If $d = m$, return $\Phi = id$.
B. Reorder $x_1, \dots, x_n$ so that:
    — $x_{d+1}, \dots, x_n$ are algebraically independent over $\mathbb{K}(\overline{f}_1, \dots, \overline{f}_d)$.
    — $x_1, \dots, x_d$ are algebraic over $\mathbb{K}(\overline{f}_1, \dots, \overline{f}_d, x_{d+1}, \dots, x_n)$.
C. For each $i \in \{1, \dots, d\}$ let

        $P_i(\overline{f}_1, \dots, \overline{f}_d, x_{d+1}, \dots, x_n) \in \mathbb{K}[\overline{f}_1, \dots, \overline{f}_d, x_{d+1}, \dots, x_n, z]$

  be non-constant and such that $P_i(\overline{f}_1, \dots, \overline{f}_d, x_{d+1}, \dots, x_n, x_i) = 0$. Let $f$ be
  a common denominator for $\overline{f}_1, \dots, \overline{f}_d$ and write $P_i = \frac{\widetilde{P}_i}{f^{r_i}}$ for adequate $r_i$'s.
```

Let $\nu = \max\{\deg\ \widetilde{P}_i,\ \deg\ f,\ n\} + 1$.

D. *Let* φ *be the monomorphism*

$$\begin{aligned} \varphi : \mathbb{K}(f_1, \ldots, f_m) &\longrightarrow \quad \mathbb{K}(x_1, \ldots, x_{n-1}) \\ f_i(x_1, \ldots, x_n) &\ \rightarrow\ f_i(x_1, \ldots, x_{n-1}, x_1^\nu) \end{aligned}$$

Let $\Phi = \varphi \circ id$.

E. *If* $m-1 = d$ *return* Φ *after undoing the reorder of the variables. Otherwise, repeat steps* B *to* E *for* $\Phi(\overline{f}_1), \ldots, \Phi(\overline{f}_m)$.

Analysis: Computing the elements in A can be done due to a constructive proof of Noether's Normalization Lemma. For step B it suffices to use Corollary 1. About the definition of φ, the conditions on ν being greater than deg f, m and each deg $\widetilde{P}_i$ ensure that the application is well defined and is a monomorphism.

It is clear that the functions $f_1, \ldots, f_m$ and $\varphi(\overline{f}_1), \ldots, \varphi(\overline{f}_m)$ have the same properties as in A.

Regarding the complexity of the algorithm, it is dominated by the computation of Gröbner bases in B; if we work in a general $\mathbb{K}$-algebra instead of a rational field, the computation of the transcendence degree according to Subsection 2.2 also needs Gröbner bases. ■

We have proved that for a certain ν, the homomorphism

$$(x_1, \ldots, x_n) \rightarrow (x_1, \ldots, x_{n-1}, x_1^\nu)$$

is a monomorphism when restricted to $\mathbb{K}(f_1, \ldots, f_m)$. Let's see that we can use this to find intermediate fields.

Theorem 19 *Assume* char $\mathbb{K} = 0$. *Let* $f \in \mathbb{K}(\mathbf{x})$ *be algebraic over* $\mathbb{K}(f_1, \ldots, f_m)$. *Then the application* Φ *that appears in Algorithm 4 is also a monomorphism when we extend it to* $\mathbb{F}$.

Proof: As the extension is separable, we can write $\mathbb{F} = \mathbb{K}(f_1, \ldots, f_m, f)$. Applying this algorithm to this representation of $\mathbb{K}$, in step A we can take the same $\overline{f}_1, \ldots, \overline{f}_d$ as for $\mathbb{K}(f_1, \ldots, f_m)$ and, as there exists $g \in \mathbb{K}(f_1, \ldots, f_m)$ such that hg is integral over $\mathbb{K}[\overline{f}_1, \ldots, \overline{f}_d]$, we take $\overline{f}_{m+1} = hg$. It is clear then that in steps B and C we can reorder the variables and take the same polynomials. From this we deduce that the value of ν that we had for $\mathbb{K}(f_1, \ldots, f_m)$ in step D is also good for $\mathbb{F}$, and the same application is a monomorphism when extended to $\mathbb{F}$. ■

Due to this result, it is enough to apply the algorithm to the given field, then we will have an algebraic extension $\mathbb{K}(\Phi(f_1), \ldots, \Phi(f_m)) \subset \mathbb{K}(x_{i_1}, \ldots, x_{i_d})$. The problem lies in how to compute $\Phi^{-1}(\mathbb{E})$ for an intermediate field in this extension, as showed in the next elementary example.

Example 6 *Let* $\Phi : \mathbb{K}(x, y, z) \to \mathbb{K}(x, y)$ *defined as*

$$\Phi(x) = x, \ \Phi(y) = y, \ \Phi(z) = x^5.$$

Let $f = y^2 \in \mathbb{K}(x, y)$*, then*

$$\left\{ \frac{x^{5n}}{z^n} y^2 + (z - x^5) \cdot g : \ n \in \mathbb{Z}, g \in \mathbb{K}(x, y, z) \right\} \subset \Phi^{-1}(f).$$

As there can be infinitely many candidates to inverse image of an element, we cannot directly check them all. To complete this solution, we would have to find a way to choose an algebraic inverse image over $\mathbb{K}(f_1, \ldots, f_m)$.

4.4 An idea based on a theorem by Schicho

Another possible method for reducing the problem to another one in an algebraic extension is based on rewriting the extension as a simple extension,

$$\begin{aligned}
&\mathbb{K}(f_1, \ldots, f_m) = \mathbb{K}(\widehat{f_1}, \ldots, \widehat{f_t})(f), \\
&\mathbb{F} = \mathbb{K}(\widehat{f_1}, \ldots, \widehat{f_t})(h), \\
&\mathbb{K}(\mathbf{x}) = \mathbb{K}(\widehat{f_1}, \ldots, \widehat{f_t}, \widehat{f_{t+1}}, \ldots, \widehat{f_n})(g),
\end{aligned}$$

where $\{\widehat{f_1}, \ldots, \widehat{f_t}\}$ is a transcendence basis of $\mathbb{K}(f_1, \ldots, f_m)$ and $\{\widehat{f_1}, \ldots, \widehat{f_n}\}$ is one of de $\mathbb{K}(\mathbf{x})$.

If we denote $\mathbb{E} = \mathbb{K}(\widehat{f_1}, \ldots, \widehat{f_t})$ and $\{\widehat{f_{t+1}}, \ldots, \widehat{f_n}\} = \{z_1, \ldots, z_k\}$, we have the fields

$$\mathbb{E}(f) \subset \mathbb{E}(h) \subset \mathbb{E}(z_1, \ldots, z_k, g)$$

so we are in the transcendence degree one case, with the exception of working in a field where the variables are not independent. The transcendence degree has been studied previously, see (Gutierrez, Rubio and Sevilla, 2001).

In order to solve this with these techniques, we would need to adapt Theorem 3 in (Schicho, 1995) to the field $\mathbb{E}(z_1,\ldots,z_k,g)$ in the following way:

Conjecture 1 *Let $A=\mathbb{K}(\mathbf{x})$ and $B=\mathbb{K}(\mathbf{y})$ two $\mathbb{K}$-algebras. Let $f_1,h_1\in A$ and $f_2,h_2\in B$ be non-constant rational functions. Then these statements are equivalent:*

(i) *There exists a rational function $g\in\mathbb{K}(t)$ such that $f_1=g(h_1)$ and $f_2=g(h_2)$.*
(ii) *h_1-h_2 divides f_1-f_2 in $A\otimes_{\mathbb{K}}B$.*

5 $\mathbb{K}$-algebras

Lastly, in this section we will briefly comment how to manipulate the elements involved from a computational point of view when we work in a field of type $QF\left(\mathbb{K}[\mathbf{x}]/I\right)$ for some prime ideal $I\subset\mathbb{K}[\mathbf{x}]$ that is given explicitly by means of a finite set of generators I.

The following known result asserts that any subfield in a finite extension is finitely generated. A proof for zero characteristic fields is due to E. Noether, Noether (1915).

Theorem 20 *Let $\mathbb{K}\subset\mathbb{K}(z_1,\ldots,z_n)$ be a finite extension. If $\mathbb{F}$ is a field such that $\mathbb{K}\subsetneq\mathbb{F}\subset\mathbb{K}(z_1,\ldots,z_n)$, then there exist $h_1,\ldots,h_s\in\mathbb{K}(z_1,\ldots,z_n)$ such that $\mathbb{F}=\mathbb{K}(h_1,\ldots,h_s)$.*

As in previous sections, all the decision problems and computation of the transcendence degree can be done for $\mathbb{K}$-algebras, see Theorem 4.

On the other hand, as the extension $\mathbb{K}\subset QF\left(\mathbb{K}[\mathbf{x}]/I\right)$ is not transcendental in general, we need to ask that it is separable. We also can adapt Subsection 2.2 to this situation. Basically, we need to add the system of generators of the ideal I to C in Theorem 5 and Corollary 2. We illustrate this with the following example.

Example 7 *We will work in the following field, which has transcendence degree 2 over $\mathbb{Q}$:*

$$\mathbb{Q}(x,y,z)=QF(\mathbb{Q}[X,Y,Z]/(X^2+Y^2)).$$

Let $f_1=(x+2y-z)^3$, $f_2=(x+2y-z)^2$ in $\mathbb{Q}(x,y,z)$. We will compute the transcendence degree of $\mathbb{Q}(f_1,f_2)$ over $\mathbb{Q}$.

A set of generators of the extended ideal is:

$$\begin{aligned}&\{F_1 = (X+2Y-Z)^3 - (x+2y-z)^3,\\ &F_2 = (X+2Y-Z)^2 - (x+2y-z)^2,\\ &P = X^2+Y^2\}.\end{aligned}$$

Deriving with respect to X, Y, Z and evaluating in x, y, z we obtain

$$\begin{pmatrix} 3\,(x+2\,y-z)^2 & 6\,(x+2\,y-z)^2 & -3\,(x+2\,y-z)^2 \\ 2\,x+4\,y-2\,z & 4\,x+8\,y-4\,z & -2\,x-4\,y+2\,z \\ 2\,x & 2\,y & 0 \end{pmatrix}$$

After some operations (remember that we are working in a $\mathbb{Q}$-algebra, so we must check that any element we want to divide by is not zero, that is, it is not in the ideal of relations) we reach an equivalent matrix:

$$\begin{pmatrix} 0 & 0 & -3(x+2\,y-z)^2 \\ 0 & 0 & -2(x+2\,y-z)^2 \\ 2\,x & 2\,y & 0 \end{pmatrix}$$

It has rank 2, so $\mathrm{tr.deg.}(\mathbb{Q}(x,y,z)/\mathbb{Q}(f_1,f_2))$ *and* $\mathrm{tr.deg.}(\mathbb{Q}(f_1,f_2)/\mathbb{Q})$ *are both 1. Also, the element x and the element y are transcendence bases of $\mathbb{Q}(x,y,z)$ over $\mathbb{Q}(f_1,f_2)$.*

Also in Subsection 4.1 we work in a setting that is general enough.

Once we reduce the problem to the algebraic case, we must consider the rest of the algorithm. If we want to use the techniques developed in Section 3 we must first ask that the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(f_1,\ldots,f_m)$ is separable.

Remark 2 *It is enough that $\mathbb{K}(\mathbf{x})/\mathbb{K}$ is separable. Indeed, then for each intermediate field $\mathbb{F}$ there exists a separating basis B such that $\mathbb{K}(B) \subset \mathbb{F}$ is algebraic separable; then we only have to find the fields in $\mathbb{K}(\mathbf{x})$ and algebraic over $\mathbb{K}(B)$, and decide which ones contain $\mathbb{F}$. To this end we will use Theorem 4 to decide if the primitive element for each field is in $\mathbb{F}$.*

About factorization in algebraic extensions and decomposition blocks, we can work in a $\mathbb{K}$-algebra in the same way as a rational field. However, the complexity increases dramatically, because of two reasons: we must manipulate the representations of the elements; and all the checks of type $f = 0$ are transformed into membership problems, $f \in \mathcal{B}_{\mathbb{K}(\mathbf{x})/\mathbb{K}}$, that demand Gröbner bases computations.

6 Conclusions

We have presented algorithms for resolving several issues related to rational function field. Our approach has combined useful computational algebra tools. Many interesting questions remain unsolved. Unfortunately, we do not know if the computed intermediate field is rational or not. The reason is that the algorithm produce an intermediate field generated always by the transcendence degree plus one elements. It should be interesting to investigate under which circumstances our algorithm can display an intermediate subfield generated by as many elements as the transcendence degree. From a more practical point of view, we would like to have either a good algorithm or a good implementation to compute a factorization of a polynomial over an algebraic extension. Concerning applications, we suggest the possible use of our techniques in the factorization of morphisms and regular maps between affine and projective algebraic sets.

References

C. Alonso, J. Gutiérrez, T. Recio, *A rational function decomposition algorithm by near-separated polynomials*. J. Symbolic. Comput. 19 (1995), no. 6, 527–544.

C. Alonso, J. Gutiérrez, R. Rubio, *On the dimension and the number of parameters of a unirational variety*. Proceedings of CCNT'99, Singapore, 3–9, Progr. Comput. Sci. Appl. Logic, 20, Birkhäuser, Basel, 2001.

M. F. Atiyah, I. G. MacDonald, *Introduction to commutative algebra*. Addison Wesley, 1969.

T. Becker, V. Weispfenning, *Groebner bases. A computational approach to commutative algebra* . In cooperation with Heinz Kredel. Graduate Texts in Mathematics, 141. Springer-Verlag, New York, 1993.

J. Brennan, W. Vasconcelos, *Effective computation of the integral closure of a morphism*. J. Pure Appl. Algebra 86 (1993), no. 2, 125–134.

D. Casperson, D. Ford, and J. McKay. *Ideal decompositions and subfields*. J. Symbolic Comput. 21 (1996), no. 2, 133–137.

J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*. Cambridge University Press, New York, 1999.

P. Gianni, B. Trager, *Integral closure of Noetherian rings*. Proceedings of ISSAC'97 (Kihei, HI), 212–216 (electronic), ACM Press, New York, 1997.

J. Gutiérrez, R. Rubio, D. Sevilla, *Unirational fields of transcendence degree one and functional decomposition.* ISSAC 2001, London, Canada, 167–174.

J. Gutiérrez, R. Rubio, D. Sevilla, *On multivariate rational function decomposition.* Computer algebra (London, ON, 2001). J. Symbolic Comput. 33 (2002), no. 5, 545–562.

G. Hommel, P. Kovács, *Simplification of symbolic inverse kinematic transformations through functional decomposition.* Proc. of the Conference Adv. in Robotics, Ferrara, 88–95 (1992).

J. Klüners, M. Pohst, *On computing Subfields.* J. of Symbolic Computation, 24 (1997), 385–397.

S. Landau, *Factoring polynomials over algebraic number fields.* SIAM J. Comput. 14 (1985), no. 1, 184–195.

S. Landau, G. L. Miller, *Solvability by radicals is in polynomial time.* J. Comput. System Sci. 30 (1985), no. 2, 179–208.

Lang, S. *Algebra.* Addison–Wesley, Reading, Mass (1967).

D. Lazard, A. Valibouze, *Computing subfields: reverse of the primitive element problem.* Computational algebraic geometry (Nice, 1992), 163–176, Progr. Math., 109, Birkhäuser Boston, Boston, MA, 1993.

A. K. Lenstra, H. W. Lenstra, L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann. 261 (1982), no. 4, 515–534.

Loos, R. *Computing in algebraic extensions.* Computer algebra, Springer, Vienna, 1983.

J. Müller-Quade, R. Steinwandt, *Basic algorithms for rational function fields.* J. Symbolic Comput. 27 (1999), no. 2, 143–170.

M. Nagata, *Theory of commutative fields.* Translations of Mathematical Monographs, 125. American Mathematical Society, Providence, RI, 1993.

E. Noether, *Körper und Systeme rationaler Funktionen.* Math. Ann. **76**, 161–196 (1915).

R. Rubio, *Unirational fields. Theorems, algorithms and applications.* PhD. Thesis. Dep. of Mathematics, University of Cantabria, Spain, 2001

I.R. Shafarevich, *Basic Algebraic Geometry.* Springer Study Edition, Springer-Verlag, 1977.

J. Schicho, *A note on a theorem of Fried and MacRae.* Arch. Math. 65, 239-243, 1995.

A. Schinzel, *Selected topics on polynomials.* Ann Arbor, University of Michigan Press, 1982.

A. Seidenberg, *Construction of the integral closure of a finite integral domain. II.* Proc. Amer. Math. Soc. 52 (1975), 368–372.

R. Steinwandt, *On computing a separating transcendence basis.* SIGSAM Bulletin, 34(4): 3-6, 2000.

M. Sweedler, *Using Gröbner bases to determine the algebraic and transcendental nature of field extensions: return of the killer tag variables.* Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), 66–75, Lecture Notes in Comput. Sci., 673, Springer, Berlin, 1993.

B. Trager, *Algebraic factoring and rational function integration.* Proc. 1976

ACM Symp. Symbolic 6 Algebraic Comp., 219–228, 1976.

W. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*. Vol. 2 of Algorithms and Computation in Mathematics, Springer-Verlag, 1998.

B. L. van der Waerden, *Modern Algebra*. Frederick Ungar Publishing Co., New York, 1964.

A. Weil, *Foundations of Algebraic Geometry*. American Mathematical Society Colloquium Publications, vol. 29. American Mathematical Society, New York, 1946.

H. Wielandt, *Finite permutation groups*. Academic Press, New York, London, 1964.

K. Yokoyama, M. Noro, T. Takeshima, *Computing primitive elements of extensions fields*. J. Symbolic Comput. 8 (1989), no. 6, 553–580.

R. Zippel, *Rational function decomposition*. Proc. ISSAC'91, ACM press, 1991.

R. Zippel, *Effective polynomial computation*. Kluwer Academic Press, 1993.