J. Symbolic Computation (2000) **30**, 469–490
doi:10.1006/jsco.1999.0417
Available online at http://www.idealibrary.com on IDEAL

Gröbner Bases Applied to Finitely Generated Field Extensions

JÖRN MÜLLER-QUADE AND RAINER STEINWANDT

Institut für Algorithmen und Kognitive Systeme, Prof. Dr. Th. Beth, Arbeitsgruppe Computeralgebra, Fakultät für Informatik, Universität Karlsruhe, Germany

Using a constructive field-ideal correspondence it is shown how to compute the transcendence degree and a (separating) transcendence basis of finitely generated field extensions $k(\vec{x})/k(\vec{g})$, resp. how to determine the (separable) degree if $k(\vec{x})/k(\vec{g})$ is algebraic. Moreover, this correspondence is used to derive a method for computing minimal polynomials and deciding field membership. Finally, a connection between certain intermediate fields of $k(\vec{x})/k(\vec{g})$ and a minimal primary decomposition of a suitable ideal is described. For Galois extensions the field-ideal correspondence can also be used to determine the elements of the Galois group.

1. Introduction

Let $k(\vec{x}) := k(x_1, \ldots, x_n)$ be a finitely generated extension field of some field k, and denote by $k(\vec{g}) := k(g_1, \ldots, g_r)$ an intermediate field of $k(\vec{x})/k$ generated over k by some elements $g_1, \ldots, g_r \in k(\vec{x})$. So geometrically, we may take $\vec{g}$ for rational functions on the variety determined by the generic point $(\vec{x})$.

To determine whether the extension $k(\vec{x})/k(\vec{g})$ is transcendental or algebraic and compute the transcendental/algebraic degree of this extension one can use Gröbner basis techniques involving so-called *tag variables* (see Kemper, 1993; Sweedler, 1993). The same techniques can also be applied to decide whether an element $f \in k(\vec{x})$ is algebraic over $k(\vec{g})$, and in the affirmative to find its minimal polynomial, for instance. For $k(\vec{x})/k$ being purely transcendental with transcendence basis $\{\vec{x}\}$, an alternate solution of these problems has been suggested in Müller-Quade and Steinwandt (1999). This approach is also based on Gröbner basis techniques, but in contrast to Sweedler (1993) and Kemper (1993) does not use tag variables. Due to the sensitivity of Buchberger's algorithm to the number of variables involved, a generalization of these techniques to the case of not necessarily purely transcendental extensions $k(\vec{x})/k$ is desirable. Some results in this direction have been given in Müller-Quade *et al.* (1998).

The aim of the present paper is to show that in fact most of the algorithms and results in Müller-Quade and Steinwandt (1999) can be extended to the situation where $k(\vec{x})/k$ is not necessarily purely transcendental. The key to the algorithms discussed is a correspondence between fields and certain ideals in polynomial rings. This correspondence can be made constructive by the use of Gröbner basis techniques.

To derive the main results we use an approach which differs from the one in Müller-Quade and Steinwandt (1999) and Müller-Quade *et al.* (1998), as this allows less technical

0747–7171/00/100469 + 22 $35.00/0

proofs. In more detail, this paper suggests solutions of the following problems (none of these solutions use tag variables).

(i) Compute the transcendence degree of $k(\vec{x})/k(\vec{g})$ and a transcendence basis of the extension $k(\vec{x})/k(\vec{g})$, which is separating if $k(\vec{x})/k(\vec{g})$ is separably generated.
(ii) For $k(\vec{x})/k(\vec{g})$ algebraic, compute the degree and separable degree of this extension.
(iii) Decide for $f \in k(\vec{x})$ whether $f \in k(\vec{g})$ or $f \notin k(\vec{g})$.
(iv) Decide for $f \in k(\vec{x})$ whether f is algebraic over $k(\vec{g})$ and in the affirmative find the minimal polynomial of f over $k(\vec{g})$.
(v) For $k(\vec{x})/k(\vec{g})$ being Galois, compute the elements of $\mathrm{Gal}(k(\vec{x})/k(\vec{g}))$.

Moreover, a connection between certain intermediate fields of $k(\vec{x})/k(\vec{g})$ and a minimal primary decomposition of a suitable ideal is described. In the last section tag variables are used to characterize all representations an element $f \in k(\vec{g})$ has in terms of given generators $\vec{g}$, thereby also obtaining another possibility for computing minimal polynomials and solving the field-membership problem.

2. A Constructive Field-Ideal Correspondence

As in the introduction we denote by $k(\vec{x}) := k(x_1, \ldots, x_n)$ a finitely generated extension field of some (ground) field k, and by $k(\vec{g}) := k(g_1, \ldots, g_r)$ the intermediate field of $k(\vec{x})/k$ generated by $g_1, \ldots, g_r \in k(\vec{x})$. For algorithmic purposes we assume computations in $k(\vec{x})$ to be effective and a finite generating set of $\mathfrak{P}_{(\vec{x})/k} := \{p(\vec{Z}) \in k[\vec{Z}] : p(\vec{x}) = 0\}$ to be known.[†] By means of a Gröbner basis of this ideal we can in particular test whether a polynomial (or rational) expression in terms of the generators $\vec{x}$ is equal to zero.

In order to tackle problems like determining the transcendence degree of $k(\vec{x})/k(\vec{g})$ it is helpful to take $k(\vec{x})$ for an extension field of $k(\vec{g})$—instead of regarding $k(\vec{g})$ as a subfield of $k(\vec{x})$. Namely, we want to express $k(\vec{x})$ as the quotient field of an integral domain $k(\vec{g})[Z_1, \ldots, Z_n]/\mathfrak{P}$ where $\mathfrak{P}$ is a prime ideal. As already noted in van der Waerden (1926) we can use the prime ideal

$$\mathfrak{P}_{(\vec{x})/k(\vec{g})} := \{p(Z_1, \ldots, Z_n) \in k(\vec{g})[Z_1, \ldots, Z_n] : p(x_1, \ldots, x_n) = 0\}$$

for this purpose.

In van der Waerden (1926) it is shown that the transcendence degree of $k(\vec{x})/k(\vec{g})$ coincides with the depth resp. dimension of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$. To turn this observation into an algorithm for computing the transcendence degree $\mathrm{transdeg}(k(\vec{x})/k(\vec{g}))$ we want to compute a finite generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$. If a finite generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ is known we can derive its dimension—and therewith $\mathrm{transdeg}(k(\vec{x})/k(\vec{g}))$—by means of a Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (see Section 3).

In a first step we determine a generating set of the extension

$$\mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})} := \mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{g})[\vec{Z}]_{\mathfrak{P}_{(\vec{x})/k(\vec{g})}}$$

of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ where as usual $k(\vec{g})[\vec{Z}]_{\mathfrak{P}_{(\vec{x})/k(\vec{g})}}$ denotes the localization of $k(\vec{g})[Z_1, \ldots, Z_n]$ at the multiplicative submonoid $k(\vec{g})[Z_1, \ldots, Z_n] \setminus \mathfrak{P}_{(\vec{x})/k(\vec{g})}$. We have the following easy to remember characterization:

[†] The notation $\mathfrak{P}_{(\vec{x})/k}$ for this ideal is adopted from Weil (1946).

Proposition 1. *Let $g_1(\vec{Z}),\dots,g_r(\vec{Z}) \in k(\vec{Z})$ be representations of $g_1,\dots,g_r \in k(\vec{x})$ in terms of $\vec{x}$, i.e. $g_i = g_i(\vec{x})$ for $i = 1,\dots,r$. Then*

$$\mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})} = \langle g_1(\vec{Z}) - g_1(\vec{x}),\dots,g_r(\vec{Z}) - g_r(\vec{x})\rangle + \langle \mathfrak{P}_{(\vec{x})/k}\rangle.$$

Proof. "$\supseteq$": Write $g_i(\vec{Z}) = \frac{n_i(\vec{Z})}{d_i(\vec{Z})}$ with $n_i(\vec{Z}) \in k[\vec{Z}]$, $d_i(\vec{Z}) \in k[\vec{Z}] \setminus \mathfrak{P}_{(\vec{x})/k}$. As $n_i(\vec{Z}) - g_i(\vec{x}) \cdot d_i(\vec{Z}) \in \mathfrak{P}_{(\vec{x})/k(\vec{g})}$ the claim follows from the equality $g_i(\vec{Z}) - g_i(\vec{x}) = d_i(\vec{Z})^{-1} \cdot (n_i(\vec{Z}) - g_i(\vec{x}) \cdot d_i(\vec{Z}))$.

"$\subseteq$": Set $\mathfrak{I} := \langle g_1(\vec{Z}) - g_1(\vec{x}),\dots,g_r(\vec{Z}) - g_r(\vec{x})\rangle + \langle \mathfrak{P}_{(\vec{x})/k}\rangle$, and let $\frac{n(\vec{Z})}{d(\vec{Z})} \in \mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})}$ with $n(\vec{Z}) \in k(\vec{g})[\vec{Z}]$, $d(\vec{Z}) \in k(\vec{g})[\vec{Z}] \setminus \mathfrak{P}_{(\vec{x})/k(\vec{g})}$. Then for suitable $\alpha \in k[\vec{g}]$, $\tilde{n}(\vec{Z}) \in k[\vec{g}][\vec{Z}]$ we can write $n(\vec{Z}) = \alpha^{-1}\tilde{n}(\vec{Z})$, and as $\mathfrak{I}$ is closed under multiplication with $\alpha^{-1}d(\vec{Z})^{-1}$, for proving $\frac{n(\vec{Z})}{d(\vec{Z})} \in \mathfrak{I}$ it is sufficient to check $\tilde{n}(\vec{Z}) \in \mathfrak{I}$. Let

$$\tilde{n}(\vec{Z}) = \tilde{n}(\vec{Z},\vec{g}(\vec{x})) = \sum_{\vec{\mu}\in\mathbb{N}^n,\vec{\nu}\in\mathbb{N}^r} \alpha_{\vec{\mu}\vec{\nu}} \cdot \prod_{i=1}^{n} {Z_i}^{\mu_i} \cdot \prod_{j=1}^{r} g_j(\vec{x})^{\nu_j} =: \sum \alpha_{\vec{\mu}\vec{\nu}} \cdot \vec{Z}^{\vec{\mu}} \cdot \prod g_j(\vec{x})^{\nu_j}$$

where $\alpha_{\vec{\mu}\vec{\nu}} \in k$ and the summations are finite. By assumption we have $\tilde{n}(\vec{x},\vec{g}(\vec{x})) = 0 \in k(\vec{x})$. Replacing each occurrence of x_i by Z_i in this equation yields $\tilde{n}(\vec{Z},\vec{g}(\vec{Z})) = 0 \in \mathrm{Quot}(k[\vec{Z}]/\mathfrak{P}_{(\vec{x})/k})$, i.e. for some $p \in \mathfrak{P}_{(\vec{x})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{x})/k}} \subseteq k(\vec{g})[\vec{Z}]_{\mathfrak{P}_{(\vec{x})/k(\vec{g})}}$ we have

$$\sum \alpha_{\vec{\mu}\vec{\nu}} \cdot \vec{Z}^{\vec{\mu}} \cdot \prod g_j(\vec{Z})^{\nu_j} = p.$$

Hence

$$\sum \alpha_{\vec{\mu}\vec{\nu}} \cdot \vec{Z}^{\vec{\mu}} \cdot \prod \left(g_j(\vec{x}) + (g_j(\vec{Z}) - g_j(\vec{x}))\right)^{\nu_j} = p,$$

and by expanding the products we obtain

$$\underbrace{\sum \alpha_{\vec{\mu}\vec{\nu}} \cdot \vec{Z}^{\vec{\mu}} \cdot \prod g_j(\vec{x})^{\nu_j}}_{=\tilde{n}(\vec{Z})} + \sum a_l \cdot (g_j(\vec{Z}) - g_j(\vec{x})) = p \tag{2.1}$$

for suitable $a_l \in k[\vec{g}(\vec{x}),\vec{g}(\vec{Z}),\vec{Z}]$. So we have $\tilde{n}(\vec{Z}) \in \mathfrak{I}$ as required. □

Before giving a method for computing a finite generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ we remind the reader that the *stable quotient* of an ideal $\mathfrak{I} \trianglelefteq k[\vec{Z}]$ w.r.t. a polynomial $q \in k[\vec{Z}]$ is the ideal $\mathfrak{I} : q^\infty := \{p \in k[\vec{Z}] : q^\mu p \in \mathfrak{I} \text{ for some } \mu \in \mathbb{N}\}$. Given $0 \neq q$ and a finite generating set of $\mathfrak{I}$ the stable quotient can be computed by means of a Gröbner basis computation in $k[Y,\vec{Z}]$ with Y a new indeterminate (Becker and Weispfenning, 1993, Proposition 6.37), i.e. the Gröbner basis computation involves $n+1$ variables. Alternatively one can use iterated ideal quotients in order to avoid the introduction of the new indeterminate Y (Alonso *et al.*, 1995). For actual computations it is also worth recalling the simple fact that the stable quotient of $\mathfrak{I}$ w.r.t. q coincides with the stable quotient of $\mathfrak{I}$ w.r.t. q' if the square-free parts of q and q' are equal—this observation can sometimes be used to decrease the degrees of the polynomials involved in the computation.

By means of the proof of Proposition 1 we can easily derive the following description of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (see also Müller-Quade *et al.*, 1998, Proposition 1):

Corollary 2. *Let $g_1(\vec{Z}), \dots, g_r(\vec{Z})$ be as in Proposition 1, and for $i = 1, \dots, r$ write $g_i = \frac{n_i(\vec{Z})}{d_i(\vec{Z})}$ with $n_i(\vec{Z}) \in k[\vec{Z}]$, $d_i(\vec{Z}) \in k[\vec{Z}] \setminus \mathfrak{P}_{(\vec{x})/k}$. Then*

$$\mathfrak{P}_{(\vec{x})/k(\vec{g})} = \left(\langle n_1(\vec{Z}) - g_1(\vec{x}) \cdot d_1(\vec{Z}), \dots, n_r(\vec{Z}) - g_r(\vec{x}) \cdot d_r(\vec{Z})\rangle + \langle \mathfrak{P}_{(\vec{x})/k}\rangle\right) : \left(\prod_{i=1}^{r} d_i(\vec{Z})\right)^{\infty} .$$

Proof. "$\supseteq$": Since $n_i(\vec{x}) - g_i(\vec{x}) \cdot d_i(\vec{x}) = 0$ for all i each polynomial $p(\vec{Z})$ contained in the stable quotient satisfies $(\prod_{i=1}^{r} d_i(\vec{x}))^{\mu} \cdot p(\vec{x}) = 0$ for some natural number μ, and from $\prod_{i=1}^{r} d_i(\vec{x}) \neq 0$ we may conclude that $p(\vec{Z}) \in \mathfrak{P}_{(\vec{x})/k(\vec{g})}$.

"$\subseteq$": Let $n(\vec{Z}) \in \mathfrak{P}_{(\vec{x})/k(\vec{g})}$. As in the proof of Proposition 1 we can write $n(\vec{Z}) = \alpha^{-1}\tilde{n}(\vec{Z})$ for suitable $\alpha \in k[\vec{g}]$, $\tilde{n}(\vec{Z}) \in k[\vec{g}][\vec{Z}]$, and we only have to verify that $\tilde{n}(\vec{Z})$ is contained in the stable quotient. Proceeding exactly as in the proof of Proposition 1 we derive the following equation (which has been labeled (2.1) above):

$$\tilde{n}(\vec{Z}) + \sum a_l \cdot (g_j(\vec{Z}) - g_j(\vec{x})) = p$$

where $p \in \mathfrak{P}_{(\vec{x})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{x})/k}}$ and the a_l are contained in $k[\vec{g}(\vec{x}), \vec{g}(\vec{Z}), \vec{Z}]$. Multiplying this equation with a suitable power of $\prod_{i=1}^{r} d_i(\vec{Z})$ we obtain

$$\left(\prod_{i=1}^{r} d_i(\vec{Z})\right)^{\mu} \cdot \tilde{n}(\vec{Z}) + \sum \tilde{a}_l \cdot (n_j(\vec{Z}) - g_j(\vec{x}) \cdot d_j(\vec{Z})) = \tilde{p} \qquad (2.2)$$

where $\mu \in \mathbb{N}$, $\tilde{p} \in \mathfrak{P}_{(\vec{x})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{x})/k}}$ and the $\tilde{a}_l$ are contained in $k(\vec{g})[\vec{Z}]$.

By construction the left-hand side of (2.2) is a polynomial in $\vec{Z}$ and vanishes when specializing $\vec{Z}$ to $\vec{x}$. So the right-hand side must also be a polynomial in $\vec{Z}$, and by construction all coefficients of this polynomial are contained in k. Therefore $\tilde{p} \in \mathfrak{P}_{(\vec{x})/k}$, i.e. we are done. □

We illustrate Corollary 2 by the simple

Example 3. Denote by $s_1, \dots, s_4$ the elementary symmetric polynomials in the indeterminates $x_1, \dots, x_4$, and set $v := \prod_{1 \le i < j \le 4}(x_i - x_j)$. Then $\mathbb{Q}(s_1, \dots, s_4, v)$ is equal to $\mathbb{Q}(x_1, \dots, x_4)^{A_4}$, the field of invariants of the alternating group A_4 acting on $\mathbb{Q}(\vec{x})$ by permutation of the indeterminates. Alternatively, $\mathbb{Q}(s_1, \dots, s_4, v)$ can be written as the quotient field of $\mathbb{Q}[S_1, \dots, S_4, V]/\mathfrak{P}_{(\vec{s},v)/\mathbb{Q}}$ where $\mathfrak{P}_{(\vec{s},v)/\mathbb{Q}}$ is the ideal generated by the discriminant relation $V^2 - \mathrm{Discr}_Z(Z^4 - S_1Z^3 + S_2Z^2 - S_3Z + S_4)$ (cf. Kemper, 1993, Section 2.3).

Now consider the subfield $\mathbb{Q}(g_1, g_2)$ of $\mathbb{Q}(s_1, \dots, s_4, v)$ with

$$(g_1, g_2) := \left({s_1}^2 - s_4, s_2 \cdot v\right) .$$

As g_1 and g_2 are polynomials, the saturation "$\dots : (\prod_i d_i)^{\infty}$" in Corollary 2 can be omitted, and we obtain the following generating set of $\mathfrak{P}_{(\vec{s},v)/k(\vec{g})}$:

$$\left\{{S_1}^2 - S_4 - ({s_1}^2 - s_4), S_2V - s_2v, V^2 - \mathrm{Discr}_Z(Z^4 - S_1Z^3 + S_2Z^2 - S_3Z + S_4)\right\} .$$

In general, Corollary 2 enables us to derive from a given tuple of generators $(\vec{g})$ of $k(\vec{g})$ a finite generating set of the ideal $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (and thereby also for the extension $\mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})}$).

The next proposition says that conversely from any finite generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ we can construct a finite tuple of generators of $k(\vec{g})$. There is no analogous statement for the ideal $\mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})}$:

Example 4. Let $\operatorname{char}(k) \neq 2$, x transcendental over k, $g := x^2$, $h := x^4$. Then by Proposition 1 we have $\mathfrak{P}^{\mathrm{e}}_{(x)/k(g)} = \langle Z^2 - x^2 \rangle$ and $\mathfrak{P}^{\mathrm{e}}_{(x)/k(h)} = \langle Z^4 - x^4 \rangle$. However, as $Z^2 + x^2 \notin \mathfrak{P}_{(x)/k(h)}$ we can also choose $Z^2 - x^2 = \frac{Z^4 - x^4}{Z^2 + x^2}$ as a generator of $\mathfrak{P}^{\mathrm{e}}_{(x)/k(h)}$. So if we know the generator $Z^2 - x^2$ only, we cannot distinguish between $k(g)$ and $k(h)$.

Proposition 5. *Let $\mathcal{P} \subseteq k(\vec{g})[\vec{Z}]$ be a generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$, and k' the field generated over k by the union of the coefficients of the polynomials in $\mathcal{P}$. Then $k' = k(\vec{g})$.*

Proof. The inclusion $k' \subseteq k(\vec{g})$ is trivial. To prove the converse inclusion we first choose a finite subset $\mathcal{P}'$ of $\mathcal{P}$ with $\langle \mathcal{P}' \rangle = \mathfrak{P}_{(\vec{x})/k(\vec{g})}$, and then apply Buchberger's algorithm to $\mathcal{P}'$ in order to derive a Gröbner basis $\mathcal{G}$ of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$. As Buchberger's algorithm does not involve any operation which requires an extension of the ground field, $\mathcal{G}$ is contained in $k'[\vec{Z}]$.

Now let $g(\vec{x}) = n(\vec{x})/d(\vec{x}) \in k(\vec{g})$ be arbitrary where $n(\vec{Z}), d(\vec{Z}) \in k[\vec{Z}] \setminus \mathfrak{P}_{(\vec{x})/k}$. Then one easily verifies that for λ transcendental over k' the normal form $N(\lambda)$ of $n(\vec{Z}) - \lambda \cdot d(\vec{Z})$ modulo $\mathcal{G}$ (taking $\mathcal{G}$ for a subset of $k'(\lambda)[\vec{Z}]$) is a linear polynomial in λ and vanishes when substituting $g(\vec{x})$ for λ (Müller-Quade *et al.*, 1998, Remark 1). Say, $N(\lambda) = a(\vec{Z}) \cdot \lambda - b(\vec{Z})$ and $a(\vec{Z}) \cdot g(\vec{x}) - b(\vec{Z}) = 0$ where $a(\vec{Z}), b(\vec{Z}) \in k'[\vec{Z}]$. To conclude that $a(\vec{Z}) \neq 0$ we can use that $n(\vec{Z}) \notin \mathfrak{P}_{(\vec{x})/k}$. Hence we obtain $g(\vec{x}) = b(\vec{Z})/a(\vec{Z})$, and since all the coefficients on the right-hand side of this equation are contained in k' we are done. □

Corollary 6. *Let $\mathcal{P}$ be the union of the finitely many reduced Gröbner bases of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$. Then the set of coefficients of the polynomials in $\mathcal{P}$ forms a finite generating set of $k(\vec{g})$ over k which for fixed generators $\vec{x}$ of $k(\vec{x})$ over k is uniquely determined by $k(\vec{g})$. Moreover, $\mathcal{P}$ can be computed effectively.*

Proof. By Proposition 5 the coefficients of the polynomials in $\mathcal{P}$ generate $k(\vec{g})$; uniqueness follows from the uniqueness of reduced Gröbner bases. For the fact that the number of reduced Gröbner bases is finite and that all of these can be computed from any finite generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (which we can obtain via Corollary 2) see Becker and Weispfenning (1993, p. 515). □

In Corollary 6 note that as $\mathcal{P}$ is the union of all reduced Gröbner bases, it is independent of the choice of a term order.

The set of intermediate fields $\mathcal{K} := \{k' \subseteq k(\vec{x}) : k' \text{ is an intermediate field of } k(\vec{x})/k\}$ has a natural lattice structure (set theoretic inclusion as partial order, intersection resp. compositum as meet resp. join). To equip the partially ordered set $\mathfrak{P}_{(\vec{x})/\mathcal{K}} := \{\mathfrak{P}_{(\vec{x})/k'} : k' \in \mathcal{K}\}$ with a lattice structure we define the meet of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ and $\mathfrak{P}_{(\vec{x})/k(\vec{h})}$ as their *set theoretic* intersection $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cap \mathfrak{P}_{(\vec{x})/k(\vec{h})} = \mathfrak{P}_{(\vec{x})/k(\vec{g}) \cap k(\vec{h})}$ (to form this intersection we take both $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ and $\mathfrak{P}_{(\vec{x})/k(\vec{h})}$ as *subsets* of $k(\vec{x})[\vec{Z}]$); for the join of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ and $\mathfrak{P}_{(\vec{x})/k(\vec{h})}$ we use the ideal $\mathfrak{P}_{(\vec{x})/k(\vec{g},\vec{h})}$ which corresponds to the compositum $k(\vec{g})k(\vec{h})$.

We can summarize the results of this section in

Theorem 7. *With the above notation*

$$\begin{array}{rccc} \mathfrak{P}_{(\vec{x})/\cdot}: & \mathcal{K} & \longrightarrow & \mathfrak{P}_{(\vec{x})/\mathcal{K}} \\ & k(\vec{g}) & \longmapsto & \mathfrak{P}_{(\vec{x})/k(\vec{g})} \end{array}$$

is a lattice-isomorphism. Moreover, $\mathfrak{P}_{(\vec{x})/\cdot}$ and its inverse can be evaluated effectively.

Proof. Bijectivity of $\mathfrak{P}_{(\vec{x})/\cdot}$ is trivial. Moreover, for $k(\vec{g}), k(\vec{h}) \in \mathcal{K}$ with $k(\vec{g}) \subseteq k(\vec{h})$ we obviously have $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \subseteq \mathfrak{P}_{(\vec{x})/k(\vec{h})}$, i.e. $\mathfrak{P}_{(\vec{x})/\cdot}$ is isotone.

In the same way we recognize the inverse of $\mathfrak{P}_{(\vec{x})/\cdot}$ as isotone: $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \subseteq \mathfrak{P}_{(\vec{x})/k(\vec{h})}$ certainly implies $k(\vec{g}) \subseteq k(\vec{h})$. So we may conclude from Birkhoff (1993, Chapter II, Section 3, Lemma 2) that $\mathfrak{P}_{(\vec{x})/\cdot}$ is a lattice isomorphism.

The effectivity of the evaluation of $\mathfrak{P}_{(\vec{x})/\cdot}$ and its inverse follows from Corollary 2 and Proposition 5: All the computations involved when computing the stable quotient in Corollary 2 by means of Buchberger's algorithm can be regarded as computations in $k(\vec{x})$, and we have assumed computations in $k(\vec{x})$ to be effective. □

When computing a Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ via Corollary 2 it is sometimes desirable to express the coefficients of the Gröbner basis explicitly as rational functions in terms of the original generators $g_1, \ldots, g_r$ of $k(\vec{g})$ (see, e.g. Section 6). To accomplish this without the introduction of additional (tag) variables one can make use of tag parameters which essentially means to keep track of how the coefficients are computed (see Müller-Quade *et al.*, 1998; Müller-Quade and Steinwandt, 1999).

3. Computing a (separating) Transcendence Basis

In this section we want to explain in more detail how a Gröbner basis of the ideal $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ can be used to compute transdeg$(k(\vec{x})/k(\vec{g}))$ and to determine a transcendence basis of this extension. Thereafter, we look at the problem of deciding whether $k(\vec{x})/k(\vec{g})$ is separably generated and computing a separating transcendence basis of this extension if there is one.

First we note that Algorithm 2 of Müller-Quade and Steinwandt (1999) can be extended to the more general situation considered here. Using the present notation it is given as Algorithm 8 below. In this algorithm $\mathrm{T}(\vec{Z})$ denotes the set of monic monomials (terms) in the variables $\vec{Z}$ and $\mathrm{HT}(p)$ denotes the leading (head) term of the polynomial p w.r.t. the term order used.

Algorithm 8.

```
In:  $\mathcal{G}$: a Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (cf. Corollary 2) w.r.t. any term order
Out: $\mathcal{B}$: a transcendence basis of $k(\vec{x})$ over $k(\vec{g})$
     $\mathcal{B} \leftarrow \emptyset$
     for $i \in \{1, \ldots, n\}$ do
       if $\mathrm{T}(\{Z_j : x_j \in \mathcal{B} \cup \{x_i\}\}) \cap \mathrm{HT}(\mathcal{G}) = \emptyset$
         then $\mathcal{B} \leftarrow \mathcal{B} \cup \{x_i\}$
     return $\mathcal{B}$
```

We have the following

Theorem 9. *Algorithm* 8 *computes a transcendence basis* $\mathcal{B}$ *of* $k(\vec{x})$ *over* $k(\vec{g})$. *In particular* $\operatorname{transdeg}(k(\vec{x})/k(\vec{g})) = |\mathcal{B}|$.

Proof. If $\mathcal{B}$ is the set returned by the algorithm then by construction $\{Z_i : x_i \in \mathcal{B}\}$ is a maximal strongly independent subset of $\{\vec{Z}\}$ modulo $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$, and since $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ is prime any maximal subset of $\{\vec{Z}\}$ strongly independent modulo $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ is also maximal independent modulo $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (this is conjectured in Kredel and Weispfenning, 1988 and proven in Kalkbrener and Sturmfels, 1995). Hence with Becker and Weispfenning (1993, Lemma 7.25) we may conclude that the residue classes of the Z_i where $x_i \in \mathcal{B}$ form a transcendence basis of $\operatorname{Quot}(k[\vec{Z}]/\mathfrak{P}_{(\vec{x})/k(\vec{g})})$ over $k(\vec{g})$, i.e. $\mathcal{B}$ is a transcendence basis of $k(\vec{x})$ over $k(\vec{g})$. □

To illustrate Algorithm 8 and Theorem 9 we can use the following small

Example 10. Let $\{x_1, x_2, x_3\}$ be algebraically independent over $\mathbb{F}_4$, and set

$$(g_1, g_2, g_3) := \left({x_1}^2 + x_2, \frac{x_2}{x_3}, \frac{{x_1}^4{x_2}^2 + {x_1}^2{x_3}^2 + {x_2}^4 + x_2{x_3}^2}{x_2x_3}\right).$$

By means of Corollary 2 and a computer algebra system like MAGMA (Bosma *et al.*, 1997) we obtain the following reduced Gröbner basis $\mathcal{G}$ of $\mathfrak{P}_{(\vec{x})/\mathbb{F}_4(\vec{g})}$ w.r.t. the graded reverse lexicographic term order where $Z_1 > Z_2 > Z_3$:

$$\mathcal{G} = \left\{{Z_1}^2 + \frac{x_2}{x_3} \cdot Z_3 + {x_1}^2 + x_2, Z_2 + \frac{x_2}{x_3} \cdot Z_3\right\}.$$

So $\operatorname{HT}(\mathcal{G}) = \{{Z_1}^2, Z_2\}$, and Algorithm 8 yields the transcendence basis $\mathcal{B} = \{x_3\}$ of $\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g})$. In particular we have $\operatorname{transdeg}(\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g})) = |\mathcal{B}| = 1$.

It is worth remarking that in this example the coefficients of the elements in $\mathcal{G}$ form a minimal generating set of $\mathbb{F}_4(\vec{g})$ over $\mathbb{F}_4$: Since $\operatorname{transdeg}(\mathbb{F}_4(\vec{g})/\mathbb{F}_4) = \operatorname{transdeg}(\mathbb{F}_4(\vec{x})/\mathbb{F}_4) - \operatorname{transdeg}(\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g})) = 3 - 1 = 2$ at least two generators are required, and by Proposition 5 the coefficients occurring in $\mathcal{G}$ form a generating set of $\mathbb{F}_4(\vec{g})$ over $\mathbb{F}_4$.

In case of $\operatorname{char}(k) > 0$ one can ask whether the extension $k(\vec{x})/k(\vec{g})$ admits a separating transcendence basis, i.e. a transcendence basis $\mathcal{B}$ of $k(\vec{x})/k(\vec{g})$ such that $k(\vec{x})/k(\vec{g})(\mathcal{B})$ is separable. Knowing a finite generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ and the transcendence degree of $k(\vec{x})/k(\vec{g})$ we can answer this question by means of a criterion from Weil (1946).

Theorem 11. (Weil, 1946, Chapter I, Theorem 2) *Let* $\mathcal{P} \subseteq k(\vec{g})[\vec{Z}]$ *be a finite generating set of* $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ *and* $t = \operatorname{transdeg}(k(\vec{x})/k(\vec{g}))$. *Then the following statements are equivalent:*

(i) $k(\vec{x})/k(\vec{g})$ *is separably generated.*
(ii) $n - t = \operatorname{rank}\left(\left(\frac{\partial p}{\partial Z_i}(\vec{x})\right)_{p\in\mathcal{P}, i=1,\ldots,n}\right)$.

Inspecting the proof of this theorem we also obtain a possibility to explicitly determine a separating transcendence basis of $k(\vec{x})/k(\vec{g})$ if there is one:

Corollary 12. *Keeping the notation of Theorem* 11 *let* $k(\vec{x})/k(\vec{g})$ *be separably generated, and select subsets* $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{I} \subseteq \{1,\ldots,n\}$ *with* $|\mathcal{P}'| = |\mathcal{I}| = n - t$ *such that* $\det\Big(\Big(\frac{\partial p}{\partial Z_i}(\vec{x})\Big)_{p\in\mathcal{P}',i\in\mathcal{I}}\Big) \neq 0$.

Then the x_i *with* $i \notin \mathcal{I}$ *form a separating transcendence basis of* $k(\vec{x})/k(\vec{g})$.

Proof. The corollary follows immediately from the proof of Weil (1946, Chapter I, Theorem 2). □

Example 13. We want to apply Theorem 11 and its corollary to the extension from Example 10. Using the Gröbner basis $\mathcal{G}$ from Example 10 as the generating set of $\mathfrak{P}_{(\vec{x})/\mathbb{F}_4(\vec{g})}$ we have to consider the following 2×3 matrix with coefficients in $\mathbb{F}_4(x_1, x_2, x_3)$:

$$\begin{pmatrix} 0 & 0 & \frac{x_2}{x_3} \\ 0 & 1 & \frac{x_2}{x_3} \end{pmatrix}.$$

Obviously this matrix is of rank two; so from $\operatorname{transdeg}(\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g})) = 1$ and Theorem 11 we conclude that the extension $\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g})$ is separably generated. Moreover, by Corollary 12 we can choose $\{x_1\}$ as a separating transcendence basis of this extension. Note that the transcendence basis $\{x_3\}$ which we have used in Example 10 is not separating; in Example 16 below we will verify that the algebraic extension $\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g}, x_3)$ is in fact of degree two and purely inseparable.

If the extension $k(\vec{x})/k(\vec{g})$ is algebraic it is natural to ask for the degree $[k(\vec{x}) : k(\vec{g})]$ of this extension; in positive characteristic also the question for the separable degree $[k(\vec{x}) : k(\vec{g})]_{\mathrm{s}}$ of $k(\vec{x})$ over $k(\vec{g})$ arises. These questions are discussed in the next section.

4. Determining the (separable) Degree of an Algebraic Extension

If $k(\vec{x})/k(\vec{g})$ is algebraic and separable, determining the degree $[k(\vec{x}) : k(\vec{g})]$ reduces to determining a primitive element of this extension and finding the degree of its minimal polynomial. We will return to this idea in Section 6 where we look at the problem of computing minimal polynomials.

In general $k(\vec{x})/k(\vec{g})$ need not be separable. To determine $[k(\vec{x}) : k(\vec{g})]$ and $[k(\vec{x}) : k(\vec{g})]_{\mathrm{s}}$ in this situation we can use a minimal Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ w.r.t. a lexicographic term order. If the known generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (cf. Corollary 2) already is a Gröbner basis w.r.t. a different term order one can apply Gröbner basis conversion techniques (see Collart *et al.*, 1997 Amrhein and Gloor, 1998 and the references therein).

We have the following generalization of Müller-Quade and Steinwandt (1999, Lemma 2.3) (for an analogous result when working with tag variables see also Kemper, 1993, Theorem 1):

Proposition 14. *Let* $k(\vec{x})/k(\vec{g})$ *be algebraic,* $\mathcal{G}$ *a minimal Gröbner basis of* $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ *w.r.t. a lexicographic term order with* $Z_1 < \cdots < Z_n$*, and for each* $i = 1,\ldots,n$ *choose a polynomial* $m_i(Z_1,\ldots,Z_i) \in \mathcal{G} \cap k[Z_1,\ldots,Z_i]$ *of minimal positive degree in* Z_i.

Then up to a constant factor in $k(\vec{g})(x_1,\ldots,x_{i-1})$ *the minimal polynomial of* x_i *over* $k(\vec{g})(x_1,\ldots,x_{i-1})$ *equals* $m_i(x_1,\ldots,x_{i-1},Z_i)$.

Proof. We can adapt the proof of Müller-Quade and Steinwandt (1999, Lemma 2.3):

Let $i \in \{1, \dots, n\}$ be arbitrary but fixed, and denote by $p(Z_i)$ the minimal polynomial of x_i over $k(\vec{g})(x_1, \dots, x_{i-1})$. Then $p(Z_i)$ can be written in the form $p(Z_i) = {Z_i}^{\alpha} + n(x_1, \dots, x_{i-1}, Z_i)/d(x_1, \dots, x_{i-1})$ where $\alpha \in \mathbb{N}$, $n(Z_1, \dots, Z_i) \in k(\vec{g})[Z_1, \dots, Z_i]$, $d(Z_1, \dots, Z_{i-1}) \in k(\vec{g})[Z_1, \dots, Z_{i-1}] \setminus \mathfrak{P}_{(x_1,\dots,x_{i-1})/k(\vec{g})}$, and the degree of $n(Z_1, \dots, Z_i)$ as a polynomial in Z_i is $< \alpha$.

In particular $\tilde{p}(Z_1, \dots, Z_i) := ({Z_i}^{\alpha} + n(Z_1, \dots, Z_i)/d(Z_1, \dots, Z_{i-1})) \cdot d(Z_1, \dots, Z_{i-1})$ is contained in $\mathfrak{P}_{(x_1,\dots,x_i)/k(\vec{g})}$ and therefore must reduce to zero modulo the Gröbner basis $\mathcal{G} \cap k(\vec{g})[Z_1, \dots, Z_i]$. Moreover, $\tilde{p}(Z_1, \dots, Z_i) \notin \mathfrak{P}_{(x_1,\dots,x_{i-1})/k(\vec{g})} \cdot k(\vec{g})[Z_1, \dots, Z_i]$, because the leading coefficient of $\tilde{p}(Z_1, \dots, Z_i)$ as a polynomial in Z_i is $d(Z_1, \dots, Z_{i-1})$ and $d(x_1, \dots, x_{i-1}) \neq 0$. We may conclude that $\tilde{p}(Z_1, \dots, Z_i)$ does not reduce to zero modulo $\mathcal{G} \cap k(\vec{g})[Z_1, \dots, Z_{i-1}]$ and that the reduction of $\tilde{p}(Z_1, \dots, Z_i)$ modulo $\mathcal{G}$ involves a polynomial in $\mathcal{G} \cap k(\vec{g})[Z_1, \dots, Z_i]$ of positive degree $\leq \alpha$ in Z_i.

Let $g(Z_1, \dots, Z_i) \in \mathcal{G} \cap k(\vec{g})[Z_1, \dots, Z_i]$ be of minimal positive degree in Z_i. From the minimality of $\mathcal{G}$ we know that the leading coefficient of $g(Z_1, \dots, Z_i)$ as an element of $k(\vec{g})[Z_1, \dots, Z_{i-1}][Z_i]$ is not contained in $\mathfrak{P}_{(x_1,\dots,x_{i-1})/k(\vec{g})}$. Hence $0 \neq g(x_1, \dots, x_{i-1}, Z_i)$, and the minimal polynomial $p(Z_i)$ of x_i is a divisor of $g(x_1, \dots, x_{i-1}, Z_i)$. As also by construction the degree of $g(x_1, \dots, x_{i-1}, Z_i)$ in Z_i is $\leq \alpha$ the polynomials $p(Z_i)$ and $g(x_1, \dots, x_{i-1}, Z_i)$ can only differ by a factor in $k(\vec{g})(x_1, \dots, x_{i-1})$. □

Corollary 15. *With the notation of Proposition* 14 *denote by α_i the degree of $m_i(Z_i)$ in Z_i, and let $r_i := \max\{r \in \mathbb{N}_0 : \exists \tilde{m} \in k(\vec{g})[Z_i]$ with $m_i(Z_i) = \tilde{m}(Z^{p^r})\}$ if $\operatorname{char}(k) = p > 0$ and $r_i := 0$, otherwise $(i = 1, \dots, n)$.*

Then $[k(\vec{x}) : k(\vec{g})] = \prod_{i=1}^{n} \alpha_i$ and $[k(\vec{x}) : k(\vec{g})]_{\mathrm{s}} = \prod_{i=1}^{n} (\alpha_i / p^{r_i})$.

Proof. The formula for the algebraic degree is a trivial consequence of Proposition 14; the formula for the separable degree follows by means of Bosch (1993, p. 111, Lemma 6), for instance. □

We can apply the above results to verify our claim of Example 13.

Example 16. We have stated that the extension $\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g}, x_3)$ (notation as in Example 13) is of degree two and purely inseparable. To verify this we can make use of Proposition 14 resp. Corollary 15:

Using the lexicographic term order with $Z_1 < Z_2 < Z_3$ MAGMA computes the following reduced (and hence in particular minimal) Gröbner basis of $\mathfrak{P}_{(\vec{x})/\mathbb{F}_4(\vec{g},x_3)}$:

$$\{{Z_1}^2 + {x_1}^2, Z_2 + x_2, Z_3 + x_3\}.$$

So according to Corollary 15 we have

$$[\mathbb{F}_4(\vec{x}) : \mathbb{F}_4(\vec{g}, x_3)] = 1 \cdot 1 \cdot 2 = 2$$

and

$$[\mathbb{F}_4(\vec{x}) : \mathbb{F}_4(\vec{g}, x_3)]_{\mathrm{s}} = \frac{1}{2^0} \cdot \frac{1}{2^0} \cdot \frac{2}{2^1} = 1.$$

In other words, the extension $\mathbb{F}_4(\vec{x})/\mathbb{F}_4(\vec{g}, x_3)$ is in fact of degree two and purely inseparable.

A more complex example where the use of Proposition 14 resp. Corollary 15 proves to be more efficient than an approach based on tag variables is discussed in more detail in the next section. Other examples where computing without tag variables is more efficient than applying an algorithm using tag variables can be found in Müller-Quade and Steinwandt (1999, Section 5).

5. An Example from Invariant Theory

Let G be the subgroup of $\mathrm{GL}_n(\mathbb{C})$ generated by the two matrices

$$\begin{pmatrix} \zeta_{31} & 0 \\ 0 & -\zeta_{31} \end{pmatrix}, \begin{pmatrix} 0 & \zeta_{31} \\ {\zeta_{31}}^{8} & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$$

where ζ_{31} denotes a primitive root of unity of order 31. One can show that G is isomorphic to the direct product of the cyclic group of order 31 with the dihedral group of order 8. In particular G consists of 248 elements and for x_1, x_2 transcendental over $\mathbb{Q}(\zeta_{31})$ operates on $\mathbb{Q}(\zeta_{31})(x_1, x_2)$ via

$$g \cdot f(x_1, x_2) := f(g_{00} \cdot x_1 + g_{01} \cdot x_2, g_{10} \cdot x_1 + g_{11} \cdot x_2) \qquad ((g_{ij})_{0 \leq i,j \leq 1} \in G).$$

Using MAGMA we can determine generators for the field of invariants $\mathbb{Q}(\zeta_{31})(x_1, x_2)^G$ over $\mathbb{Q}(\zeta_{31})$; we have $\mathbb{Q}(\zeta_{31})(x_1, x_2)^G = \mathbb{Q}(\zeta_{31})(g_1(\vec{x}), \ldots, g_{17}(\vec{x}))$, where the $g_i(\vec{x})$ are defined as follows:

$$\begin{pmatrix} g_1(\vec{x}) \\ g_2(\vec{x}) \\ g_3(\vec{x}) \\ g_4(\vec{x}) \\ g_5(\vec{x}) \\ g_6(\vec{x}) \\ g_7(\vec{x}) \\ g_8(\vec{x}) \\ g_9(\vec{x}) \\ g_{10}(\vec{x}) \\ g_{11}(\vec{x}) \\ g_{12}(\vec{x}) \\ g_{13}(\vec{x}) \\ g_{14}(\vec{x}) \\ g_{15}(\vec{x}) \\ g_{16}(\vec{x}) \\ g_{17}(\vec{x}) \end{pmatrix} = \begin{pmatrix} {x_1}^{62} + {x_2}^{62} \\ {x_1}^{60}{x_2}^{2} + {\zeta_{31}}^{1}4{x_1}^{2}{x_2}^{60} \\ {x_1}^{58}{x_2}^{4} + {\zeta_{31}}^{28}{x_1}^{4}{x_2}^{58} \\ {x_1}^{56}{x_2}^{6} + {\zeta_{31}}^{11}{x_1}^{6}{x_2}^{56} \\ {x_1}^{54}{x_2}^{8} + {\zeta_{31}}^{25}{x_1}^{8}{x_2}^{54} \\ {x_1}^{52}{x_2}^{10} + {\zeta_{31}}^{8}{x_1}^{10}{x_2}^{52} \\ {x_1}^{50}{x_2}^{12} + {\zeta_{31}}^{22}{x_1}^{12}{x_2}^{50} \\ {x_1}^{48}{x_2}^{14} + {\zeta_{31}}^{5}{x_1}^{14}{x_2}^{48} \\ {x_1}^{46}{x_2}^{16} + {\zeta_{31}}^{19}{x_1}^{16}{x_2}^{46} \\ {x_1}^{44}{x_2}^{18} + {\zeta_{31}}^{2}{x_1}^{18}{x_2}^{44} \\ {x_1}^{42}{x_2}^{20} + {\zeta_{31}}^{16}{x_1}^{20}{x_2}^{42} \\ {x_1}^{40}{x_2}^{22} + {\zeta_{31}}^{-1}{x_1}^{22}{x_2}^{40} \\ {x_1}^{38}{x_2}^{24} + {\zeta_{31}}^{13}{x_1}^{24}{x_2}^{38} \\ {x_1}^{36}{x_2}^{26} + {\zeta_{31}}^{27}{x_1}^{26}{x_2}^{36} \\ {x_1}^{34}{x_2}^{28} + {\zeta_{31}}^{10}{x_1}^{28}{x_2}^{34} \\ {x_1}^{32}{x_2}^{30} + {\zeta_{31}}^{24}{x_1}^{30}{x_2}^{32} \\ {x_1}^{124} + {x_2}^{124} \end{pmatrix}.$$

According to Kemper (1994, Proposition 1.2) the extension

$$\mathbb{Q}(\zeta_{31})(x_1, x_2)/\mathbb{Q}(\zeta_{31})(x_1, x_2)^G$$

is algebraic of degree $|G| = 248$. Using MAGMA V2.4–6 and the methods described in this paper we want to verify this statement. For the computations a *Sun Ultra-5* with 333 MHz and 128 MB RAM under *SunOS Release 5.6* and *OpenWindows Version 3.6* has been used.

5.1. Computing the transcendence degree

By means of Corollary 2 we obtain the generating set

$$\{g_1(\vec{Z}) - g_1(\vec{x}), \ldots, g_{17}(\vec{Z}) - g_{17}(\vec{x})\}$$

of $\mathfrak{P}_{(x_1,x_2)/\mathbb{Q}(\zeta_{31})(x_1,x_2)^G}$ (as $g_1(\vec{x}), \ldots, g_{17}(\vec{x})$ are polynomials, the saturation can be omitted). As $\mathrm{char}(\mathbb{Q}) = 0$ we can apply Theorem 11 to compute the transcendence degree of $\mathbb{Q}(\zeta_{31})(x_1, x_2)/\mathbb{Q}(\zeta_{31})(x_1, x_2)^G$. In particular it is not necessary to apply Algorithm 8 (which requires a Gröbner basis of $\mathfrak{P}_{(x_1,x_2)/\mathbb{Q}(\zeta_{31})(x_1,x_2)^G}$) in this case.

Using MAGMA's command `Rank` the rank of the corresponding 17×2 matrix after 14.04 s computes to two (in this example it is more efficient to verify the linear independence of two rows by means of `IsIndependent`; this can be accomplished in less than 0.03 s). Hence the extension $\mathbb{Q}(\zeta_{31})(x_1, x_2)/\mathbb{Q}(\zeta_{31})(x_1, x_2)^G$ is of transcendence degree $2 - 2 = 0$, i.e. it is algebraic, and we can compute the degree of this extension.

5.2. Determining the degree

To determine the degree of $[\mathbb{Q}(\zeta_{31})(x_1, x_2) : \mathbb{Q}(\zeta_{31})(x_1, x_2)^G]$ we want to use Corollary 15. For this aim we first compute a Gröbner basis of $\mathfrak{P}_{(x_1,x_2)/\mathbb{Q}(\zeta_{31})(x_1,x_2)^G}$. To avoid unnecessary reductions during the computation of the Gröbner basis we use the command `GroebnerBasisUnreduced` provided by MAGMA. Using the graded reverse lexicographic term order with $Z_1 > Z_2$ after about 853.18 s we obtain an (already reduced) Gröbner basis $\mathcal{G}$ consisting of three polynomials where $\mathrm{HT}(\mathcal{G}) = \{{Z_2}^{64}, {Z_1}^2{Z_2}^{60}, {Z_1}^4\}$. We remark that avoiding unnecessary reductions is quite important here: Applying `GroebnerBasis` with the standard parameters takes 8715.41 s.

By means of `GroebnerWalk` (cf. Collart *et al.*, 1997) the unique reduced Gröbner basis of $\mathfrak{P}_{(\vec{x})/\mathbb{Q}(\zeta_{31})(\vec{x})^G}$ w.r.t. to the lexicographic term order with $Z_1 > Z_2$ can be derived from $\mathcal{G}$ within 1.61 s. It consists of two polynomials with leading term ${Z_1}^2$ resp. ${Z_2}^{124}$, and by means of Corollary 15 we obtain

$$[\mathbb{Q}(\zeta_{31})(x_1, x_2) : \mathbb{Q}(\zeta_{31})(x_1, x_2)^G] = 2 \cdot 124 = 248$$

as expected.

5.3. Using tag variables

To verify that the extension $\mathbb{Q}(\zeta_{31})(x_1, x_2)/\mathbb{Q}(\zeta_{31})(x_1, x_2)^G$ is algebraic of degree 248 it is also possible to use Gröbner basis techniques based on tag variables (cf. Kemper, 1993; Sweedler, 1993).

Here the ideal under consideration is

$$\langle g_1(\vec{Z}) - T_1, \ldots, g_{17}(\vec{Z}) - T_{17}\rangle \subseteq \mathbb{Q}(\zeta_{31})[Z_1, Z_2, T_1, \ldots, T_{17}].$$

We start by computing a Gröbner basis of this ideal with respect to a term order that eliminates Z_1 and Z_2 (in MAGMA the name *elim-2* is used). Using `GroebnerBasis` after about 8270.24 s yields the reduced Gröbner basis $\mathcal{G}_{\mathrm{T}}$ consisting of 228 polynomials (using `GroebnerBasisUnreduced` takes 12155.1 s; in particular this does not result in a speed-up). So the required CPU time is significantly higher than in the approach without tag variables described above.

By means of the Gröbner basis the extension $\mathbb{Q}(\zeta_{31})(x_1,x_2)/\mathbb{Q}(\zeta_{31})(x_1,x_2)^G$ is easily identified as algebraic. To derive the degree of the extension we convert $\mathcal{G}_{\mathrm{T}}$ into a Gröbner basis w.r.t. a term order where $\mathrm{T}(Z_1,Z_2)$ are ordered lexicographically. This conversion (by means of `GroebnerWalk`) provides no further difficulties and results in a Gröbner basis consisting of 229 polynomials, and by means of Kemper (1993, Proposition 2) we obtain

$$[\mathbb{Q}(\zeta_{31})(x_1,x_2):\mathbb{Q}(\zeta_{31})(x_1,x_2)^G]=2\cdot 124=248.$$

6. Minimal Polynomials and Field Membership

For computational purposes the main drawback of Proposition 14 for determining the degree of an algebraic extension is the requirement of using a lexicographic term order. For separable algebraic extensions, i.e. in particular for $\operatorname{char}(k)=0$, the procedure described below can be applied to compute $[k(\vec{x}):k(\vec{g})]$ without involving a lexicographic term order. More precisely we make use of the following remark:

Remark 17. (Lang, 1993, Chapter VIII, Exercise 5, for instance) Let $u_1,\dots,u_n$ be algebraically independent over $k(\vec{x})$ and $k(\vec{x})/k(\vec{g})$ separable algebraic. Then we have the equality $k(\vec{g})(\vec{u})(\sum_{i=1}^n u_ix_i)=k(\vec{x})(\vec{u})$.

With the notation of this remark we clearly have $[k(\vec{x}):k(\vec{g})]=[k(\vec{x})(\vec{u}):k(\vec{g})(\vec{u})]$. So for finding $[k(\vec{x}):k(\vec{g})]$ it is sufficient to compute (the degree of) the minimal polynomial of $\sum_{i=1}^n u_ix_i$ over $k(\vec{g})(\vec{u})$ (of course the minimal polynomial of a known primitive element of $k(\vec{x})/k(\vec{g})$ can serve the same purpose).

With the assumption that $x_1,\dots,x_n$ are algebraically independent over k a method for computing minimal polynomials over $k(\vec{g})$ by means of an arbitrary Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ is given by Müller-Quade and Steinwandt (1999, Algorithm 3.2). Subsequently we want to show that this procedure extends to the more general situation considered here: Let $f\in k(\vec{x})$ be algebraic over $k(\vec{g})$ with minimal polynomial $m(Z)=Z^\alpha+\sum_{i=0}^{\alpha-1}\lambda_iZ^i$ of degree $\alpha\in\mathbb{N}$, and choose polynomials $n(Z_1,\dots,Z_n)\in k[\vec{Z}]$, $d(Z_1,\dots,Z_n)\in k[\vec{Z}]\setminus\mathfrak{P}_{(\vec{x})/k}$ with $f=f(\vec{x})=n(\vec{x})/d(\vec{x})$. Then the fraction $m(n(\vec{Z})/d(\vec{Z}))$ is contained in the ideal $\mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})}$. Conversely, if for some $\gamma_j\in k(\vec{g})$, $\beta\in\mathbb{N}$ we have

$$\left(\frac{n(\vec{Z})}{d(\vec{Z})}\right)^\beta+\sum_{j=0}^{\beta-1}\gamma_j\left(\frac{n(\vec{Z})}{d(\vec{Z})}\right)^j\in\mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})}\tag{6.3}$$

then f is a root of $Z^\beta+\sum_{j=0}^{\beta-1}\gamma_jZ^j$. So to find the minimal polynomial of f over $k(\vec{g})$ it is sufficient to find the smallest $\beta\in\mathbb{N}$ and corresponding $\gamma_j\in k(\vec{g})$ such that (6.3) holds. To test for concrete values β and $\vec{\gamma}$ effectively whether (6.3) holds we can use the equivalent condition

$$d(\vec{Z})^\beta\cdot\left(\left(\frac{n(\vec{Z})}{d(\vec{Z})}\right)^\beta+\sum_{j=0}^{\beta-1}\gamma_j\left(\frac{n(\vec{Z})}{d(\vec{Z})}\right)^j\right)\in\mathfrak{P}_{(\vec{x})/k(\vec{g})}\tag{6.4}$$

(note that $d(\vec{Z})$ is a unit in $k(\vec{g})[\vec{Z}]_{\mathfrak{P}_{(\vec{x})/k(\vec{g})}}$).

Solving the ideal membership problem (6.4) reduces to the computation of a normal form modulo any Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$. Unfortunately we do not know the values of $\vec{\gamma}$ and β in advance. To overcome this difficulty we remind the reader of

Remark 18. (Müller-Quade and Steinwandt, 1999, Remark 1.4) Let $A_1, \ldots, A_l$ be new elements transcendental over $k(\vec{g})$, $\alpha_1, \ldots, \alpha_l \in k(\vec{g})$, $\mathcal{G}$ a Gröbner basis of $\langle \mathcal{G} \rangle \trianglelefteq k(\vec{g})[\vec{Z}]$ w.r.t. some term order, and $p_i(\vec{Z}) \in k(\vec{g})[Z_1, \ldots, Z_n]$, $h_i(\vec{A}) \in k(\vec{g})[\vec{A}]$ $(i = 1, \ldots, s)$.

Then specializing $A_j \mapsto \alpha_j$ $(j = 1, \ldots, l)$ in the normal form of $\sum_{i=1}^{s} h_i(\vec{A}) \cdot p_i(\vec{Z})$ modulo $\mathcal{G}$ yields the normal form of $\sum_{i=1}^{s} h_i(\vec{\alpha}) \cdot p_i(\vec{Z})$ modulo $\mathcal{G}$.

So after fixing $\beta \in \mathbb{N}$ we can decide whether there are $\vec{\gamma} \in k(\vec{g})$ such that (6.4) resp. (6.3) holds as follows:

(1) Introduce new parameters (i.e. over $k(\vec{g})$ transcendental elements) $A_0, \ldots, A_{\beta-1}$.

(2) Compute the normal form $N(\vec{Z}) \in k(\vec{g})[\vec{A}][\vec{Z}]$ of

$$d(\vec{Z})^{\beta} \cdot \left(\left(\frac{n(\vec{Z})}{d(\vec{Z})} \right)^{\beta} + \sum_{j=0}^{\beta-1} A_j \left(\frac{n(\vec{Z})}{d(\vec{Z})} \right)^{j} \right)$$

modulo some Gröbner basis $\mathcal{G}$ of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (in the computation of the normal form the $\vec{A}$ are regarded as constants, i.e. $\mathcal{G}$ is taken for a subset of $k(\vec{g})(\vec{A})[\vec{Z}]$).

(3) Solve the linear system of equations (for the indeterminates $\vec{A}$) which we obtain by equating all the coefficients of $N(\vec{Z}) \in k(\vec{g})[\vec{A}][\vec{Z}]$ to zero.

(4) For each solution $\vec{\gamma}$ of the system of equations in the previous step condition (6.4) resp. (6.3) holds. Conversely, if the equations in the previous step do not admit a solution there are no $\vec{\gamma}$ such that (6.4) resp. (6.3) holds.

To find the minimal polynomial of $f(\vec{x}) = n(\vec{x})/d(\vec{x})$ over $k(\vec{g})$ we can perform these four steps successively for $\beta = 1, 2, 3, \ldots$ until the linear system of equations in the third step has a solution (which then necessarily is contained in $k(\vec{g})$). As a by-product this also yields a field membership test for f: $f \in k(\vec{g})$ holds iff it has a linear $(\beta = 1)$ minimal polynomial over $k(\vec{g})$.

In summary we have the following analog of Müller-Quade and Steinwandt (1999, Theorem 3.1).

Theorem 19. *Let $f(\vec{x}) \in k(\vec{x})$ be algebraic over $k(\vec{g})$ and choose $n(Z_1, \ldots, Z_n) \in k[\vec{Z}]$, $d(Z_1, \ldots, Z_n) \in k[\vec{Z}] \setminus \mathfrak{P}_{(\vec{x})/k}$ such that $f(\vec{x}) = n(\vec{x})/d(\vec{x})$. Then Algorithm* 20 *computes the minimal polynomial of $f(\vec{x})$ over $k(\vec{g})$.*

Since Müller-Quade and Steinwandt (1999, Algorithm 3.2) is just a special case of Algorithm 20 we refer to Müller-Quade and Steinwandt (1999, Section 3.3) for an example which illustrates Theorem 19 resp. Algorithm 20.

Algorithm 20.

In: $\mathcal{G}$: *a Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ (cf. Corollary* 2*) w.r.t. any term order*

```
      f:    $f(\vec{x}) = \frac{n(\vec{x})}{d(\vec{x})}$ is algebraic over $k(\vec{g})$ with $n(\vec{Z})$, $d(\vec{Z})$ as in Theorem 19
Out:  $m(Z)$: the minimal polynomial of $f(\vec{x})$ over $k(\vec{g})$.
      Create a new indeterminate $Z$.
      $\beta \leftarrow 1$
      repeat
        Create a formal parameter $A_{\beta-1}$.
        $N(\vec{Z}) \leftarrow$normal form of $d(\vec{Z})^{\beta} \cdot \left( \left( \frac{n(\vec{Z})}{d(\vec{Z})} \right)^{\beta} + \sum_{j=0}^{\beta-1} A_j \left( \frac{n(\vec{Z})}{d(\vec{Z})} \right)^{j} \right)$ modulo $\mathcal{G}$
        $\mathcal{C} \leftarrow$ the set of coefficients of $N(\vec{Z}) \in k(\vec{g})[\vec{A}][\vec{Z}]$
        $\mathcal{A} \leftarrow \{(\gamma_0, \ldots, \gamma_{\beta-1}) \in k(\vec{g}) | \forall c(\vec{A}) \in \mathcal{C} : c(\gamma_0, \ldots, \gamma_{\beta-1}) = 0\}$
        if $\mathcal{A} \neq \emptyset$
          then select $(\gamma_0, \ldots, \gamma_{\beta-1}) \in \mathcal{A}$
               $m(Z) \leftarrow Z^{\beta} + \sum_{j=0}^{\beta-1} \gamma_j Z^j$
        $\beta \leftarrow \beta + 1$
      until $\mathcal{A} \neq \emptyset$
      return $m(Z)$
```

As already mentioned in Section 2 if one is interested in expressing the coefficients of the minimal polynomial in terms of given generators $\vec{g}$ of $k(\vec{g})$ one can make use of tag parameters as discussed in Müller-Quade and Steinwandt (1999) and Müller-Quade *et al.* (1998). Finally, it is worth mentioning that Algorithm 20 cannot be used to decide whether $f(\vec{x})$ is algebraic over $k(\vec{g})$ or not. However, by means of Algorithm 8 we can determine $\text{transdeg}(k(\vec{x})/k(\vec{g}))$ and $\text{transdeg}(k(\vec{x})/k(\vec{g})(f))$; then f is algebraic over $k(\vec{g})$ iff these transcendence degrees are equal, and we can be sure that Algorithm 20 terminates in this case.

An alternate approach for deciding whether an element $f \in k(\vec{x})$ is algebraic over $k(\vec{g})$ is to determine an upper bound b for the possible degree of the minimal polynomial of f: If we know such a bound b and after b iterations of the loop in Algorithm 20 no minimal polynomial for f has been found, then f must be transcendental over $k(\vec{g})$. Of course, if we are only interested in knowing whether f is transcendental or algebraic over $k(\vec{g})$ and not in the minimal polynomial itself, it is sufficient to pass through the loop in Algorithm 20 once with $\beta = b$. By the choice of b then f is algebraic over $k(\vec{g})$ iff $\mathcal{A} \neq \emptyset$.

For $\vec{x}$ being algebraically independent over k such a bound b can be determined easily (Müller-Quade and Steinwandt, 1999, Lemma 3.4). For the more general situation considered here we still have the following bound which can be computed effectively by means of the techniques discussed in Sections 3 and 4:

Remark 21. Let $f \in k(\vec{x})$ be algebraic over $k(\vec{g})$, $\mathcal{B}$ a transcendence basis of $k(\vec{x})/k(\vec{g})$. Then $[k(\vec{g})(f) : k(\vec{g})] \leq [k(\vec{x}) : k(\vec{g})(\mathcal{B})]$.

Proof. Up to notation the same as the proof of Müller-Quade and Steinwandt (1999, Remark 3.3). □

Example 22. Let $k(\vec{x})/k(\vec{g})$ be purely transcendental, and choose $\mathcal{B}$ as a transcendence basis of $k(\vec{x})/k(\vec{g})$ with $k(\vec{x}) = k(\vec{g})(\mathcal{B})$. Then Remark 21 specializes to the well-known result that the purely transcendental extension $k(\vec{x})/k(\vec{g})$ cannot have an intermediate field k' with $k'/k(\vec{g})$ algebraic.

In dependence of the upper bound b the loop in Algorithm 20 has to be passed $\mathrm{O}(b)$ times to determine a minimal polynomial. By using a kind of binary search we can restrict ourselves to $\mathrm{O}(\log b)$ executions of the steps in the loop.

— If the loop in Algorithm 20 is entered with a value of β which is smaller than the degree of the minimal polynomial we look for, or if f is transcendental over $k(\vec{g})$, then the set of solutions $\mathcal{A}$ is empty.

— Conversely, if β is larger than the degree δ of the minimal polynomial $m(Z)$ of f then $\mathcal{A}$ contains more than one element, as for all $\alpha \in k(\vec{g})$, the polynomial $(Z-\alpha)^{\beta-\delta} \cdot m(Z)$ satisfies $\left(n(\vec{Z})/d(\vec{Z})\right)^{\beta} + \sum_{j=0}^{\beta-1} \gamma_{\alpha j} \left(n(\vec{Z})/d(\vec{Z})\right)^{j} \in \mathfrak{P}^{\mathrm{e}}_{(\vec{x})/k(\vec{g})}$ (with suitable $\gamma_{\alpha j} \in k(\vec{g})$).

In summary, we have criteria to decide whether our guess for β is too small, too large or correct (in the latter case $\mathcal{A}$ contains one unique solution, as the minimal polynomial is unique). So instead of testing successively for $\beta = 1, 2, 3, \ldots$ we can use a binary search in the set $\{1, \ldots, b\}$ to identify β.

7. Galois Extensions and Intermediate Fields

By definition an algebraic extension $k(\vec{x})/k(\vec{g})$ is Galois iff it is separable and normal. With the methods in Sections 3 and 4 we can decide effectively whether $k(\vec{x})/k(\vec{g})$ is separable algebraic. To check whether the extension is also normal—and therewith Galois—we can apply Algorithm 20 to find the minimal polynomials $m_1(Z), \ldots, m_n(Z)$ of $x_1, \ldots, x_n$ over $k(\vec{g})$; then $k(\vec{x})/k(\vec{g})$ being normal is equivalent to the condition that $\prod_{i=1}^{n} m_i(Z)$ over $k(\vec{x})$ splits into linear factors (e.g. Bosch, 1993, Section 3.5, Theorem 4).

If $k(\vec{x})/k(\vec{g})$ has been recognized as Galois the question arises how the corresponding Galois group $\mathrm{Gal}(k(\vec{x})/k(\vec{g}))$ looks. In terms of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ we can characterize $\mathrm{Gal}(k(\vec{x})/k(\vec{g}))$ via

Theorem 23. (van der Waerden, 1928, Satz 25) *Let $k(\vec{x})/k(\vec{g})$ be Galois. Then*

$$\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}] = \prod_{\sigma \in \mathrm{Gal}(k(\vec{x})/k(\vec{g}))} \langle Z_1 - \sigma(x_1), \ldots, Z_n - \sigma(x_n) \rangle .$$

From this theorem we obtain a method to determine all $\sigma \in \mathrm{Gal}(k(\vec{x})/k(\vec{g}))$:

Corollary 24. *Let the extension $k(\vec{x})/k(\vec{g})$ be Galois, $\mathfrak{P}_1, \ldots, \mathfrak{P}_l$ the associated prime ideals of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}]$, and G_i a reduced Gröbner basis of $\mathfrak{P}_i$ ($i = 1, \ldots, l$). Then*

$$\{G_1, \ldots, G_l\} = \{\{Z_1 - \sigma(x_1), \ldots, Z_n - \sigma(x_n)\} : \sigma \in \mathrm{Gal}(k(\vec{x})/k(\vec{g}))\} .$$

Proof. Since the factors in the decomposition of $\mathfrak{P}_{(\vec{x})/k(\vec{g})}$ in Theorem 23 are pairwise comaximal we have $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}] = \bigcap_{\sigma \in \mathrm{Gal}(k(\vec{x})/k(\vec{g}))} \langle Z_1 - \sigma(x_1), \ldots, Z_n - \sigma(x_n) \rangle$ which is a minimal primary decomposition of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}]$. Due to the uniqueness of the minimal primary decomposition of zero-dimensional ideals (see Becker and Weispfenning, 1993, Lemma 8.60, cf. also the more fundamental Jacobson, 1980, Theorem 7.13) the maximal ideals $\langle Z_1 - \sigma(x_1), \ldots, Z_n - \sigma(x_n)\rangle$ coincide with the associated primes of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}]$. Finally, $\{Z_1 - \sigma(x_1), \ldots, Z_n - \sigma(x_n)\}$ is a reduced Gröbner basis w.r.t. every term order, so we are done. □

To illustrate Corollary 24 through a simple example we look at the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$:

Example 25. Set $k := \mathbb{Q}$, $x_1 := \sqrt{2}$, $x_2 := \sqrt{3}$, $g_1 := 1$ (as "generator" of the trivial extension $\mathbb{Q}/\mathbb{Q}$). So we have $\mathfrak{P}_{(\vec{x})/k} = \langle {Z_1}^2 - 2, {Z_2}^2 - 3\rangle$, and from Corollary 2 we obtain $\mathfrak{P}_{(\vec{x})/k(\vec{g})} = \mathfrak{P}_{(\vec{x})/k} \cdot \mathbb{Q}[Z_1, Z_2]$. Using MAGMA again, for instance, we obtain the primary decomposition

$$\begin{aligned}\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot \mathbb{Q}(\sqrt{2}, \sqrt{3})[Z_1, Z_2] = {} & \langle Z_1 - \sqrt{2}, Z_2 - \sqrt{3}\rangle \cap \\ & \langle Z_1 - \sqrt{2}, Z_2 + \sqrt{3}\rangle \cap \\ & \langle Z_1 + \sqrt{2}, Z_2 - \sqrt{3}\rangle \cap \\ & \langle Z_1 + \sqrt{2}, Z_2 + \sqrt{3}\rangle\end{aligned}$$

where the changing signs reflect the Klein four-group structure of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.

Without the assumption that $k(\vec{x})/k(\vec{g})$ is Galois a minimal primary decomposition of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}]$ still proves useful to characterize certain intermediate fields of $k(\vec{x})/k(\vec{g})$ (for analogous statements with the restriction $k(\vec{x})/k(\vec{g})$ algebraic see Müller-Quade and Steinwandt, 1999, Lemma 4.2 and Müller-Quade *et al.*, 1998, Lemma 4):

Lemma 26. *Let $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}] = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_l$ be a minimal primary decomposition, $\mathfrak{P}_i$ the associated prime of $\mathfrak{Q}_i$ ($i = 1, \ldots, l$), $k(\vec{h})$ an intermediate field of $k(\vec{x})/k(\vec{g})$, and $k(\vec{g})^{\mathrm{alg}}$ the algebraic closure of $k(\vec{g})$ in $k(\vec{x})$. Then the following holds:*

- *(i) If $k(\vec{g})^{\mathrm{alg}}/k(\vec{h})$ is separable algebraic then $\mathfrak{P}_{(\vec{x})/k(\vec{h})} \cdot k(\vec{x})[\vec{Z}] = \bigcap_{\lambda \in \Lambda} \mathfrak{P}_\lambda$ for some $\Lambda \subseteq \{1, \ldots, l\}$.*
- *(ii) If $k(\vec{h})/k(\vec{g})$ is separable algebraic then $\mathfrak{P}_{(\vec{x})/k(\vec{h})} \cdot k(\vec{x})[\vec{Z}] = \bigcap_{\lambda \in \Lambda} \mathfrak{Q}_\lambda$ for some $\Lambda \subseteq \{1, \ldots, l\}$.*

Proof. Since $k(\vec{h})/k(\vec{g})$ is algebraic we have $\dim(\mathfrak{P}_{(\vec{x})/k(\vec{g})}) = \mathrm{transdeg}(k(\vec{x})/k(\vec{g})) = \mathrm{transdeg}(k(\vec{x})/k(\vec{h})) = \dim(\mathfrak{P}_{(\vec{x})/k(\vec{h})})$. Moreover, $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{h})[\vec{Z}] \subseteq \mathfrak{P}_{(\vec{x})/k(\vec{h})}$, so from $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{h})[\vec{Z}]$ being unmixed (Zariski and Samuel, 1960, Corollary 1, p. 225) and the fact that prime ideals of the same dimension cannot properly contain each other (Becker and Weispfenning, 1993, Lemma 7.57) we deduce that $\mathfrak{P}_{(\vec{x})/k(\vec{h})}$ is minimal among the primes in $k(\vec{h})[\vec{Z}]$ containing $\mathfrak{P}$, i.e. it is an associated prime of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{h})[\vec{Z}]$.

Now assume that $k(\vec{g})^{\mathrm{alg}}/k(\vec{h})$ is separable algebraic: Then by Zariski and Samuel (1960, Corollary, p. 226, Corollary 1, p. 225) $\mathfrak{P}_{(\vec{x})/k(\vec{h})} \cdot k(\vec{g})^{\mathrm{alg}}[\vec{Z}]$ is radical and unmixed. So all its associated primes $\mathfrak{A}_1, \ldots, \mathfrak{A}_a$ are of dimension $\dim(\mathfrak{P}_{(\vec{x})/k(\vec{h})}) = \dim(\mathfrak{P}_{(\vec{x})/k(\vec{g})})$, and using again Becker and Weispfenning (1993, Lemma 7.57) we recognize them as associated primes of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{g})^{\text{alg}}[\vec{Z}]$. Finally, as all operations required for computing the associated primes of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}]$ can take place in $k(\vec{g})^{\text{alg}}[\vec{Z}]$ (e.g. Gianni *et al.*, 1988) $\mathfrak{A}_1 \cdot k(\vec{x})[\vec{Z}], \dots, \mathfrak{A}_a \cdot k(\vec{x})[\vec{Z}]$ are associated primes of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{x})[\vec{Z}]$.

To prove (ii) assume that $k(\vec{h})/k(\vec{g})$ is separable algebraic and denote by $k(\vec{g})^{\text{sep}}$ the separable algebraic closure of $k(\vec{g})$ in $k(\vec{g})^{\text{alg}}$. Replacing $k(\vec{g})^{\text{alg}}$ with $k(\vec{g})^{\text{sep}}$ in the above argumentation we recognize $\mathfrak{P}_{(\vec{x})/k(\vec{h})}$ as the intersection of associated prime ideals $\mathfrak{B}_1, \dots, \mathfrak{B}_b$ of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{g})^{\text{sep}}[\vec{Z}]$. Since $k(\vec{g})^{\text{alg}}/k(\vec{g})^{\text{sep}}$ is purely inseparable we know from Zariski and Samuel (1960, Corollary 2, p. 225) that $\mathfrak{B}_1 \cdot k(\vec{g})^{\text{alg}}[\vec{Z}], \dots, \mathfrak{B}_b \cdot k(\vec{g})^{\text{alg}}[\vec{Z}]$ are primary. Since the same computations can be used to check minimality of a primary decomposition of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{g})^{\text{sep}}[\vec{Z}]$ and of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{g})^{\text{alg}}[\vec{Z}]$ we can conclude that $\mathfrak{B}_1 \cdot k(\vec{g})^{\text{alg}}[\vec{Z}], \dots, \mathfrak{B}_b \cdot k(\vec{g})^{\text{alg}}[\vec{Z}]$ occur in a minimal primary decomposition of $\mathfrak{P}_{(\vec{x})/k(\vec{g})} \cdot k(\vec{g})^{\text{sep}}[\vec{Z}]$. Finally, also the operations required for computing a minimal primary decomposition can take place in $k(\vec{g})^{\text{alg}}[\vec{Z}]$ (e.g. Gianni *et al.*, 1988), and hence $\mathfrak{B}_1 \cdot k(\vec{x})[\vec{Z}], \dots, \mathfrak{B}_b \cdot k(\vec{x})[\vec{Z}]$ are contained in $\{\mathfrak{Q}_1, \dots, \mathfrak{Q}_l\}$. □

As in Müller-Quade and Steinwandt (1999, Lemma 4.2) the requirements concerning separability in Lemma 26 cannot be dropped:

Example 27. (cf. Müller-Quade and Steinwandt, 1999, Section 4.2) For the purely inseparable extension $\mathbb{F}_5(x)/\mathbb{F}_5(x^{25})$ (with x transcendental over $\mathbb{F}_5$) the minimal primary decomposition of $\mathfrak{P}_{(x)/\mathbb{F}_5(x^{25})} \cdot \mathbb{F}_5(x)[Z]$ computes to

$$\left\langle Z^{25} - x^{25} \right\rangle = \left\langle Z - x \right\rangle^{25}.$$

So the proper intermediate field $\mathbb{F}_5(x^5)$ can neither be identified as an intersection of associated primes nor as an intersection of primary components.

Moreover, as in the case of purely inseparable extensions, the number of intermediate fields is not necessarily finite and we cannot hope to identify all of the intermediate fields by means of the characterization in Lemma 26 which involves only finitely many ideals.

If Lemma 26 is used to determine $\mathfrak{P}_{(\vec{x})/k(\vec{h})} \cdot k(\vec{x})[\vec{Z}]$ for some intermediate field $k(\vec{h})$ of $k(\vec{x})/k(\vec{g})$, then a given generating set of $\mathfrak{P}_{(\vec{x})/k(\vec{h})} \cdot k(\vec{x})[\vec{Z}]$ is not necessarily contained in $k(\vec{h})[\vec{Z}]$ already. However, a reduced Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{h})} \cdot k(\vec{x})[\vec{Z}]$ must be contained in $k(\vec{h})[\vec{Z}]$, because we could also have applied Buchberger's algorithm to a generating set in $k(\vec{h})[\vec{Z}]$ to derive the reduced Gröbner basis—thereby never involving elements in $k(\vec{x}) \setminus k(\vec{h})$. So from Proposition 5 we can conclude

Remark 28. The coefficients of a reduced Gröbner basis of $\mathfrak{P}_{(\vec{x})/k(\vec{h})} \cdot k(\vec{x})[\vec{Z}]$ form a generating set of $k(\vec{h})$ over k.

Before going on to the next section we want to point out two special cases of the above lemma which are immediate from the proof:

Remark 29. With the notation of Lemma 26 denote by $k(\vec{g})^{\text{sep}}$ the separable algebraic closure of $k(\vec{g})$ in $k(\vec{x})$. Then the following hold:

(i) $\mathfrak{P}_{(\vec{x})/k(\vec{g})^{\mathrm{alg}}} \cdot k(\vec{x})[\vec{Z}] = \mathfrak{P}$ for some $\mathfrak{P} \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_l\}$
(ii) $\mathfrak{P}_{(\vec{x})/k(\vec{g})^{\mathrm{sep}}} \cdot k(\vec{x})[\vec{Z}] = \mathfrak{Q}$ for some $\mathfrak{Q} \in \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_l\}$

8. Using Tag Variables to Decide Field Membership

For $f \in k(\vec{g})$ we know that there is a $q(\vec{Z}) \in k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$ such that $f = q(\vec{g})$, and as described in Section 6 we can find such a q through the use of tag parameters. In this section we give another solution to the field-membership problem, which is based on tag variables and enables us to characterize *all* possible choices of $q \in k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$ with $f = q(\vec{g})$. For this purpose we extend the method from Müller-Quade and Steinwandt (1999, Section 1.4), which is based on tag variables, to the situation considered here. For alternate solutions to the field membership involving tag variables we refer to Sweedler (1993) and Kemper (1993).

The key for characterizing all possible representations of f in terms of $\vec{g}$ is the following simple remark (cf. Müller-Quade and Steinwandt, 1999, Lemma 1.11):

Remark 30. Let $f \in k(\vec{g})$ and $q \in k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$ with $f = q(\vec{g})$. Then for $q'(\vec{Z}) \in k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$ the following statements are equivalent:

(i) $f = q'(\vec{g})$
(ii) $q - q' \in \mathfrak{P}_{(\vec{g})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$

Proof. (i)⇒(ii): We have $q'(\vec{g}) = f = q(\vec{g})$ and therefore $0 = (q - q')(\vec{g})$ resp. $q - q' \in \mathfrak{P}_{(\vec{g})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$.

(i)⇐(ii): $q - q' \in \mathfrak{P}_{(\vec{g})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$ yields $(q - q')(\vec{g}) = 0$, i.e. $q'(\vec{g}) = q(\vec{g}) = f$. □

Hence we can characterize all representations by finding one representation $q(\vec{Z})$ and a basis of $\mathfrak{P}_{(\vec{g})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$. Using tag variables $T_1, \dots, T_r$ such a basis can be found by means of the next lemma (for a proof see Müller-Quade and Rötteler, 1998, Lemma 5 and Corollary 6):

Lemma 31. *Let $g_1(\vec{Z}), \dots, g_r(\vec{Z})$ be as in Proposition 1, and for $i = 1, \dots, r$ write $g_i = \frac{n_i(\vec{Z})}{d_i(\vec{Z})}$ with $n_i(\vec{Z}) \in k[\vec{Z}]$, $d_i(\vec{Z}) \in k[\vec{Z}] \setminus \mathfrak{P}_{(\vec{x})/k}$. Then setting*

$$\mathfrak{A} := \langle n_1(\vec{Z}) - T_1 \cdot d_1(\vec{Z}), \dots, n_r(\vec{Z}) - T_r \cdot d_r(\vec{Z}) \rangle + \langle \mathfrak{P}_{(\vec{x})/k} \rangle \trianglelefteq k[\vec{T}, \vec{Z}]$$

we have the following equalities:

$$\{p(\vec{T}, \vec{Z}) : p \in \mathfrak{P}_{(\vec{g},\vec{x})/k}\} = \left(\mathfrak{A} : \left(\prod_{i=1}^{r} d_i(\vec{Z})\right)^{\infty}\right)$$

$$\{p(\vec{T}) : p \in \mathfrak{P}_{(\vec{g})/k}\} = \left(\mathfrak{A} : \left(\prod_{i=1}^{r} d_i(\vec{Z})\right)^{\infty}\right) \cap k[\vec{T}].$$

Since up to the names of the variables the sets $\{p(\vec{T}, \vec{Z}) : p \in \mathfrak{P}_{(\vec{g},\vec{x})/k}\}$ and $\{p(\vec{T}) : p \in \mathfrak{P}_{(\vec{g})/k}\}$ coincide with $\mathfrak{P}_{(\vec{g},\vec{x})/k}$ and $\mathfrak{P}_{(\vec{g})/k}$, if confusion is not likely, we will denote these sets by $\mathfrak{P}_{(\vec{g},\vec{x})/k}$ resp. $\mathfrak{P}_{(\vec{g})/k}$, too.

So using Becker and Weispfenning (1993, Proposition 6.37) and a term order with all terms in $\vec{T}$ alone being smaller than the terms containing another variable we can determine a basis of $\mathfrak{P}_{(\vec{g})/k}$—and hence in particular of $\mathfrak{P}_{(\vec{g})/k} \cdot k[\vec{Z}]_{\mathfrak{P}_{(\vec{g})/k}}$—through a Gröbner basis computation over k (involving $n+r+1$ variables). Due to the "elimination property" of Gröbner bases (see, e.g. Becker and Weispfenning, 1993, Proposition 6.15) the generating set for $\mathfrak{P}_{(\vec{g},\vec{x})/k}$ we obtain when computing the stable quotient via Becker and Weispfenning (1993, Proposition 6.37) is in fact a Gröbner basis. We want to exploit this fact to derive a solution to the field-membership problem:

Let $\pi : \; k[\vec{T}][\vec{Z}] \rightarrow \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})[\vec{Z}]$ be the canonical homomorphism mapping each T_i onto its residue class and mapping each Z_j to Z_j. With the same argumentation as in the proof of Müller-Quade and Steinwandt (1999, Lemma 1.15) we obtain

Lemma 32. *Let $\mathcal{G}$ be a Gröbner basis of $\mathfrak{P}_{(\vec{g},\vec{x})/k} \trianglelefteq k[\vec{T},\vec{Z}]$ w.r.t. a term order where each term involving only $\vec{T}$ is smaller than the terms containing another variable. Then $\pi(\mathcal{G}) \setminus \{0\}$ is a Gröbner basis of $\langle \pi(\mathfrak{P}_{(\vec{g},\vec{x})/k})\rangle \trianglelefteq \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})[\vec{Z}]$ w.r.t. the induced term order.*

Now we have all the necessary ingredients to decide for $f := n(\vec{x})/d(\vec{x}) \in k(\vec{x})$ (where $n(\vec{Z}) \in k[\vec{Z}]$ and $d(\vec{Z}) \in k[\vec{Z}] \setminus \mathfrak{P}_{(\vec{x})/k}$) whether $f \in k(\vec{g})$ holds:

The statement $f \in k(\vec{g})$ is equivalent to the statement

$$\exists c \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k}) : \; \pi(n(\vec{Z})) - c \cdot \pi(d(\vec{Z})) \in \langle \pi(\mathfrak{P}_{(\vec{g},\vec{x})/k})\rangle \tag{8.5}$$

(with $\langle \pi(\mathfrak{P}_{(\vec{g},\vec{x})/k})\rangle$ being understood as an ideal in $\mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})[\vec{Z}]$), as obviously for each $c = c(\vec{T})$ satisfying (8.5) we have $c(\vec{g}) = f$, and conversely each representation $f = c(\vec{g})$ of f in terms of $\vec{g}$ yields an element $c \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$ as required in (8.5).

So using Remark 18 we can apply the following three-step "procedure" for deciding whether $f = n(\vec{x})/d(\vec{x}) \in k(\vec{g})$ holds:

(1) Use Lemma 31 to compute a Gröbner basis $\mathcal{G}$ of $\mathfrak{P}_{(\vec{g},\vec{x})/k}$ w.r.t. a term order where all terms in $\vec{T}$ alone are smaller than the terms containing another variable.

(2) Determine the normal form $N(A)$ of $n(\vec{Z}) - A \cdot d(\vec{Z})$ modulo $\pi(\mathcal{G}) \setminus \{0\}$ where A is a new transcendental element [which is adjoined to $\mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$].

(3) Check whether the linear system of equations (in the indeterminate A) which we obtain by equating all coefficients of $N(A) \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})(A)[\vec{Z}]$ to zero has a solution c [which can be chosen from $\mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$].

While the execution of the first of these steps should not require further explanation we want to give some remarks on the second and third step:
Step 2: Taking the elements of the Gröbner basis $\mathcal{G}$ as elements of $\mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})[\vec{Z}]$ resp. $\mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})(A)[\vec{Z}]$ in the second step raises the question of recognizing vanishing coefficients: To avoid dividing by zero while computing the normal form $N(A)$ we must know which of the (leading) coefficients occurring in $\mathcal{G} \subset k[\vec{T}][\vec{Z}]$ actually represent the zero element in $\mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$.

As $\mathcal{G} \cap k[\mathrm{T}]$ is a Gröbner basis of $\mathfrak{P}_{(\vec{g})/k}$, we can check for each coefficient $c(\vec{T})$ occurring in $\mathcal{G} \subset k[\vec{T}][\vec{Z}]$ whether $\pi(c(\vec{T})) = 0$ holds by reducing it modulo $\mathcal{G} \cap k[\vec{T}]$. Of course, if $\mathcal{G}$

in the first step is chosen to be a minimal or reduced Gröbner basis none of the leading coefficients in $\mathcal{G} \subset k[\vec{T}][\vec{Z}]$ can be contained in the kernel of π, anyway.

If the correct leading coefficients in $\pi(\mathcal{G})$ are known, computing $N(A)$ is standard, as the only coefficients which have to be inverted during the reduction are the leading coefficients in $\pi(\mathcal{G})$. Note that apart from sometimes performing an "empty reduction"—when the leading coefficient of the polynomial we reduce represents $0 \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$—there is no harm if we perform the reductions in $k(\vec{T})[\vec{Z}]$, i.e. taking $\vec{T}$ for algebraically independent over k.

Step 3: Exploiting again the fact that $\mathcal{G} \cap k[\vec{T}]$ is a Gröbner basis of $\mathfrak{P}_{(\vec{g})/k}$ we can easily identify whether an expression in $\vec{T}$ represents $0 \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$, so solving the linear equations (resp. checking their solvability) is standard.

We want to point out that in Müller-Quade and Steinwandt (1999, Algorithm 1.17) a different method for checking the condition $N(A) = 0 \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$ has been suggested. An advantage of the above method is its immediate generalization to the problem of computing minimal polynomials over $k(\vec{g})$:

For $m(Z) = Z^\beta + \sum_{j=0}^{\beta-1} c_j(\vec{g}) \cdot Z^j \in k(\vec{g})[Z]$ with $m(f) = 0$ we certainly have

$$\pi(d(\vec{Z}))^\beta \cdot \left(\left(\frac{\pi(n(\vec{Z}))}{\pi(d(\vec{Z}))} \right)^\beta + \sum_{j=0}^{\beta-1} c_j \left(\frac{\pi(n(\vec{Z}))}{\pi(d(\vec{Z}))} \right)^j \right) \in \langle \pi(\mathfrak{P}_{(\vec{g},\vec{x})/k}) \rangle \tag{8.6}$$

where $c_j = c_j(\vec{T}) \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$; conversely if we find $c_j \in \mathrm{Quot}(k[\vec{T}]/\mathfrak{P}_{(\vec{g})/k})$ satisfying (8.6) then $f^\beta + \sum_{j=0}^{\beta-1} c_j(\vec{g}) \cdot f^j = 0$. To check whether such a tuple $(\vec{c})$ exists we can look at the normal form of

$$\pi(d(\vec{Z}))^\beta \cdot \left(\left(\frac{\pi(n(\vec{Z}))}{\pi(d(\vec{Z}))} \right)^\beta + \sum_{j=0}^{\beta-1} A_j \left(\frac{\pi(n(\vec{Z}))}{\pi(d(\vec{Z}))} \right)^j \right)$$

modulo a Gröbner basis of $\mathfrak{P}_{(\vec{g},\vec{x})/k}$, and the essential difference to the above steps for deciding field membership is the fact that the linear equations in the last step can involve up to β indeterminates A_j instead of one. Hence, we can proceed in a fashion completely analogous to Algorithm 20 for determining the minimal polynomial of an element $f \in k(\vec{x})$ algebraic over $k(\vec{g})$, if a Gröbner basis of $\mathfrak{P}_{(\vec{g},\vec{x})/k}$ is known.

To illustrate the use of tag variables we give an example motivated by a matrix factorization problem:

Example 33. In Aagedal *et al.* (1996) the following chain of fields was used in the context of factoring a given 2×2 matrix into a product D_1CD_2 where D_1, D_2 are diagonal matrices and C denotes a circulant matrix. It reflects the solution steps of the matrix factorization problem; the generators of the intermediate field correspond to intermediate results:

$$\underbrace{\mathbb{C}(d_1c_1d_3, d_1c_2d_4, d_2c_2d_3, d_2c_1d_4)}_{=:K} \le \underbrace{\mathbb{C}\left(\frac{c_1}{c_2}, \frac{d_3}{d_4}, \frac{d_1}{d_2}, d_1c_1d_3\right)}_{=:L} \le \mathbb{C}(d_1, d_2, d_3, d_4, c_1, c_2).$$

We use the abbreviations $(\vec{x}) := (d_1, d_2, d_3, d_4, c_1, c_2)$ and $(\vec{g}) := \left(\frac{c_1}{c_2}, \frac{d_3}{d_4}, \frac{d_1}{d_2}, d_1c_1d_3\right)$. By means of tag variables we want to determine all representations of the generators $d_1c_1d_3$,

$d_1c_2d_4$, $d_2c_2d_3$, $d_2c_1d_4$ of the field K in terms of the generators $\vec{g}$ of L: With the notation of Lemma 31 we have

$$\begin{aligned}\mathfrak{A} &:= \langle c_1 - T_1 \cdot c_2, d_3 - T_2 \cdot d_4, d_1 - T_3 \cdot d_2, d_1c_1d_3 - T_4\rangle \trianglelefteq \mathbb{C}[\vec{T}, d_1, d_2, d_3, d_4, c_1, c_2],\\ \{p(\vec{T}, \vec{Z}) &: p \in \mathfrak{P}_{(\vec{x},\vec{g})/\mathbb{C}}\} = \mathfrak{A} : (c_2d_4d_2)^\infty \trianglelefteq \mathbb{C}[\vec{T}, d_1, d_2, d_3, d_4, c_1, c_2].\end{aligned}$$

Using the lexicographic term order with

$$d_1 > d_2 > d_3 > d_4 > c_1 > c_2 > T_1 > T_2 > T_3 > T_4$$

we calculate the following Gröbner basis of $\mathfrak{P}_{(\vec{x},\vec{g})/\mathbb{C}}$:

$$\mathcal{G} := \{d_1 - T_3 \cdot d_2, T_1T_2T_3 \cdot d_2d_4c_2 - T_4, d_3 - T_2 \cdot d_4, c_1 - T_1 \cdot c_2\}\,.$$

No polynomials from $\mathbb{C}[\vec{T}]$ occur. Hence the generators of the field L are algebraically independent over $\mathbb{C}$ and the representation of the generators of K in the generators of L is unique.

Now let A be a formal parameter. The normal form of

$$d_1c_1d_3 - A$$

modulo $\mathcal{G}$ in $\mathbb{C}(T_1, T_2, T_3, T_4)(A)[d_1, d_2, d_3, d_4, c_1, c_2]$ evaluates to $T_4 - A$. Solving the equation $T_4 - A$ for A we get the expected trivial representation $d_1c_1d_3 = d_1c_1d_3$ as $d_1c_1d_3$ is already contained in the generating system of L.

For the polynomial $d_1c_2d_4$ the corresponding normal form computes to

$$\frac{T_4 - A \cdot T_1T_2}{T_1T_2},$$

i.e. we get the representation

$$d_1c_2d_4 = \frac{d_1c_1d_3}{\frac{c_1}{c_2} \cdot \frac{d_3}{d_4}}.$$

Analogously, for the polynomials $d_2c_2d_3$ and $d_2c_1d_4$ we obtain the representations

$$d_2c_2d_3 = \frac{d_1c_1d_3}{\frac{c_1}{c_2} \cdot \frac{d_1}{d_2}} \qquad \text{and} \qquad d_2c_1d_4 = \frac{d_1c_1d_3}{\frac{d_3}{d_4} \cdot \frac{d_1}{d_2}}.$$

Acknowledgements

The authors would like to thank Thomas Beth, Markus Grassl, Martin Rötteler, and two referees for helpful comments and "proofreading with the louse comb". This work was supported by grant DFG–GRK 209/3–98 "Beherrschbarkeit komplexer Systeme".

References

Aagedal, H., Beth, T., Müller-Quade, J., Schmid, M. (1996, November). Algorithmic design of diffractive optical systems for information processing. In Toffoli, T., Biafore, M., Leão, J. eds, *Proceedings of the Fourth Workshop on Physics and Computation PhysComp96*, pp. 1–6. New England Complex Systems Institute.

Alonso, C., Gutierrez, J., Recio, T. (1995). An implicitization algorithm with fewer variables. *Comput. Aided Geom. Des.*, **12**, 251–258.

Amrhein, B., Gloor, O. (1998). The fractal walk. In Buchberger, B., Winkler, F. eds, *Gröbner Bases and Applications*, volume 251 of *Lecture Note Series*, pp. 305–322. London Mathematical Society: Cambridge University Press.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases: A Computational Approach to Commutative Algebra, Graduate Texts in Mathematics.* New York, Springer.

Birkhoff, G. (1993). *Lattice Theory,* 3$^{\text{rd}}$ edn, volume 25 of *Colloquium Publications.* Providence, RI, American Mathematical Society.

Bosch, S. (1993). *Algebra.* Berlin, Springer-Lehrbuch; Heidelberg, Springer.

Bosma, W., Cannon, J., Playoust, C. (1997). The Magma algebra system I: The user language. *J. Symb. Comput.*, **24**, 235–265.

Collart, S., Kalkbrener, M., Mall, D. (1997). Converting bases with the Gröbner walk. *J. Symb. Comput.*, **24**, 465–469.

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, **6**, 149–167.

Jacobson, N. (1980). *Basic Algebra*, volume 2. San Francisco, W. H. Freeman and Company.

Kalkbrener, M., Sturmfels, B. (1995). Initial complexes of prime ideals. *Adv. Math.*, **116**, 365–376.

Kemper, G. (1993, October). An algorithm to determine properties of field extensions lying over a ground field. IWR Preprint 93-58, Heidelberg, Germany.

Kemper, G. (1994, August). Das Noethersche Problem und generische Polynome. Dissertation, Universität Heidelberg, Germany.

Kredel, H., Weispfenning, V. (1988). Computing dimension and independent sets for polynomial ideals. *J. Symb. Comput.*, **6**, 231–247.

Lang, S. (1993). *Algebra*, 3$^{\text{rd}}$ edn. Addison-Wesley Publishing Company, Inc.

Müller-Quade, J., Rötteler, M. (1998, August). Deciding linear disjointness of finitely generated fields. In Gloor, O. ed., *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, pp. 153–160. The Association for Computing Machinery, Inc. (ACM).

Müller-Quade, J., Steinwandt, R. (1999). Basic algorithms for rational function fields. *J. Symb. Comput.*, **27**, 143–170.

Müller-Quade, J., Steinwandt, R., Beth, T. (1998). An application of Gröbner bases to the decomposition of rational mappings. In Buchberger, B., Winkler, F. eds, *Gröbner Bases and Applications*, volume 251 of *Lecture Note Series*, pp. 448–462. London Mathematical Society: Cambridge University Press.

Sweedler, M. (1993). Using Gröbner bases to determine the algebraic and transcendental nature of field extensions: return of the killer tag variables. In Cohen, G., Mora, T., Moreno, O. eds, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 10th International Symposium, AAECC-10* LNCS **673**, pp. 66–75. Berlin, Heidelberg, Springer.

van der Waerden, B. L. (1926). Zur Nullstellentheorie der Polynomideale. *Math. Annal.*, **96**, 183–208.

van der Waerden, B. L. (1928). Eine Verallgemeinerung des Bézoutschen Theorems. *Math. Annal.*, **99**, 497–541.

Weil, A. (1946). *Foundations of Algebraic Geometry* (Rev. and enl. ed.), volume 29 of *Colloquium Publications.* Providence, RI, American Mathematical Society.

Zariski, O., Samuel, P. (1960). *Commutative Algebra*—volume II*, Graduate Texts in Mathematics*, New York, Heidelberg, Berlin, Springer.

Originally Received 31 January 1999
Accepted 27 July 1999