J. Symbolic Computation (1999) **27**, 143–170
Article No. jsco.1998.0246
Available online at http://www.idealibrary.com on IDEAL

Basic Algorithms for Rational Function Fields

JÖRN MÜLLER-QUADE AND RAINER STEINWANDT

Arbeitsgruppe Prof. Dr. Th. Beth, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, D-76128 Karlsruhe, Germany

By means of Gröbner basis techniques algorithms for solving various problems concerning subfields $\mathbb{K}(\mathbf{g}) := \mathbb{K}(g_1, \ldots, g_m)$ of a rational function field $\mathbb{K}(\mathbf{x}) := \mathbb{K}(x_1, \ldots, x_n)$ are derived: computing canonical generating sets, deciding field membership, computing the degree and separability degree resp. the transcendence degree and a transcendence basis of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$, deciding whether $f \in \mathbb{K}(\mathbf{x})$ is algebraic or transcendental over $\mathbb{K}(\mathbf{g})$, computing minimal polynomials, and deciding whether $\mathbb{K}(\mathbf{g})$ contains elements of a "particular structure", e.g. monic univariate polynomials of fixed degree. The essential idea is to reduce these problems to questions concerning an ideal of a polynomial ring; connections between minimal primary decompositions over $\mathbb{K}(\mathbf{x})$ of this ideal and intermediate fields of $\mathbb{K}(\mathbf{g})$ and $\mathbb{K}(\mathbf{x})$ are given. In the last section some practical considerations concerning the use of the algorithms are discussed.

0. Introduction

Rational function fields $\mathbb{K}(\mathbf{x}) := \mathbb{K}(x_1, \ldots, x_n)$ arise in various contexts within mathematics and computer science. Two examples are invariant theory (Kemper, 1994) and the design of diffractive optical systems (Aagedal *et al.*, 1996). In the latter, multivariate decomposition of rational functions proves useful for inverting rational functions.

For performing practical calculations in subfields $\mathbb{K}(\mathbf{g}) := \mathbb{K}(g_1, \ldots, g_m)$ of $\mathbb{K}(\mathbf{x})$ it is desirable to have algorithms for solving problems like field membership or the computation of a canonical generating set. The algorithms given in Sweedler (1993) and Kemper (1993) are mainly concerned with questions like calculating minimal polynomials over $\mathbb{K}(\mathbf{g})$ and finding the transcendental/algebraic degree of an extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$. In addition to these algorithms for deciding the field membership problem are given. Both Sweedler and Kemper make use of Gröbner basis techniques with the introduction of additional ("tag") variables and a lexicographical order of the terms in $\mathbf{x}$, leading to difficulties in practical computations.

The motivation of this paper on the one hand is to find alternate solutions to the problems discussed by Sweedler and Kemper in order to broaden the spectrum of effectively tractable problems; on the other hand, we want to give new algorithms for questions concerning subfields $\mathbb{K}(\mathbf{g})$. For this we associate to $\mathbb{K}(\mathbf{g})$ an ideal in the polynomial ring $\mathbb{K}(\mathbf{g})[\mathbf{Z}]$, thereby reducing problems such as computing a canonical generating set of $\mathbb{K}(\mathbf{g})$ over $\mathbb{K}$ or determining the type of the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ to problems concerning an ideal in a polynomial ring. More precisely the problems treated in the text are:

0747–7171/99/020143 + 28 $30.00/0

- Compute a finite canonical set of generators of $\mathbb{K}(\mathbf{g})$ over $\mathbb{K}$.
- Given $f \in \mathbb{K}(\mathbf{x})$ decide if $f \in \mathbb{K}(\mathbf{g})$, and in the affirmative case compute $h \in \mathbb{K}(y_1, \ldots, y_m)$ with $f = h(g_1, \ldots, g_m)$.
- Given $f \in \mathbb{K}(\mathbf{x})$ decide if $f \in \mathbb{K}(\mathbf{g})$, and in the affirmative case determine *all* $h \in \mathbb{K}(y_1, \ldots, y_m)$ with $f = h(g_1, \ldots, g_m)$.
- Compute the transcendence degree t of $\mathbb{K}(\mathbf{x})$ over $\mathbb{K}(\mathbf{g})$. In case of

  $(t = 0)$ compute the degree $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]$ and the separability degree $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]_s$;in case of
  $(t > 0)$ compute a transcendence basis of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ and decide whether this extension is separably generated. In the affirmative case choose the transcendence basis to be separating.

- Given $f \in \mathbb{K}(\mathbf{x})$ algebraic over $\mathbb{K}(\mathbf{g})$ find the minimal polynomial of f over $\mathbb{K}(\mathbf{g})$.
- Given $f \in \mathbb{K}(\mathbf{x})$ decide whether f is algebraic or transcendental over $\mathbb{K}(\mathbf{g})$.
- Given parameters $A_1, \ldots, A_v$, $f(\mathbf{A}, \mathbf{x}) \in \mathbb{K}(\mathbf{A}, \mathbf{x})$, $\mathbb{K}(\mathbf{g}) \leq \mathbb{K}(\mathbf{x})$ where $\mathbb{K}$ is algebraically closed decide if there is a specialization $(\mathbf{A}) \mapsto (\alpha_1, \ldots, \alpha_v)$, $\quad \in \mathbb{K}$ such that $f(\quad, \mathbf{x}) \in \mathbb{K}(\mathbf{g})$.

In Section 4, connections between intermediate fields of $\mathbb{K}(\mathbf{g})$ and $\mathbb{K}(\mathbf{x})$ and minimal primary decompositions over $\mathbb{K}(\mathbf{x})$ of the ideal associated to $\mathbb{K}(\mathbf{g})$ are given.

To illustrate the algorithms several examples are given throughout the paper. Moreover, the last section deals with some practical considerations concerning the use of the algorithms.

Notation

Throughout the text the following abbreviations are used:

$\mathbb{K}$	any field where calculations can be done effectively
$\mathbb{K}(\mathbf{x})$	the rational function field $\mathbb{K}(x_1, \ldots, x_n)$
$\mathbb{K}(\mathbf{g})$	the subfield $\mathbb{K}(g_1, \ldots, g_m)$ of $\mathbb{K}(x_1, \ldots, x_n)$
$\underline{Z}$	the product $Z_1 \cdot \ldots \cdot Z_n$
$\underline{\mu}$	the multi-exponent $(\mu_1, \ldots, \mu_n)$, i.e. $\underline{Z}^{\underline{\mu}} = {Z_1}^{\mu_1} \cdot \ldots \cdot {Z_n}^{\mu_n}$
$\lvert\underline{\mu}\rvert$	the weight of $\underline{\mu}$, namely $\sum_{i=1}^{n} \mu_i$
$\langle H \rangle \trianglelefteq \mathbb{K}[\mathbf{Z}]$	the ideal in the polynomial ring $\mathbb{K}[\mathbf{Z}]$ generated by $H \subseteq \mathbb{K}[\mathbf{Z}]$
$\mathrm{T}(\mathbf{x})$	the set of terms in the variables $\mathbf{x}$ (with a term being understood as a monic monomial)
$\mathrm{HT}(p)$	the head (leading) term of the polynomial p w. r. t. a specified order
$\mathrm{HC}(p)$	the head (leading) coefficient of the polynomial p w. r. t. a specified order
$\mathbf{Y} \ll \mathbf{Z}$	for $t_1 \in \mathrm{T}(\mathbf{Y}), t_2 \in \mathrm{T}(\mathbf{Y}, \mathbf{Z}) \setminus \mathrm{T}(\mathbf{Y})$ the term order $\leq$ satisfies $t_1 < t_2$
$\overline{p}$	the residue class of $p \in \mathbb{K}[\mathbf{Z}]$ modulo a given ideal
$I : p^{\infty}$	the saturation of the ideal I with respect to the polynomial p, namely the set $\{q \in \mathbb{K}[\mathbf{Z}] \mid \exists \mu \in \mathbb{N}_{>0} : p^{\mu} q \in I\}$
$\mathrm{Quot}(R)$	the quotient field of the integral domain R

1. Canonical Sets of Generators and the Field Membership Problem

The aim of this section is to give a constructive answer to

PROBLEM 1. *("canonical generating set"):*

Given $\mathbb{K}(\mathbf{g}) \leq \mathbb{K}(\mathbf{x})$ *compute a finite canonical set of generators* $\mathcal{C}(\mathbf{g})$ *of* $\mathbb{K}(\mathbf{g})$ *over* $\mathbb{K}$, *i.e.* $\mathbb{K}(\mathbf{g}) = \mathbb{K}(\mathbf{g'})$ *if and only if* $\mathcal{C}(\mathbf{g}) = \mathcal{C}(\mathbf{g'})$.

It turns out that the solution to this problem proposed below can also be used to solve

PROBLEM 2. *("field membership"):*

(A) ("non-constructive") Given $f \in \mathbb{K}(\mathbf{x})$ *decide if* $f \in \mathbb{K}(\mathbf{g})$.
(B) ("constructive") Given $f \in \mathbb{K}(\mathbf{x})$ *decide if* $f \in \mathbb{K}(\mathbf{g})$, *and in the affirmative case compute* $h \in \mathbb{K}(y_1, \ldots, y_m)$ *with* $f = h(\mathbf{g})$.

An approach to Problem 2(B) using tag variables has been given in Sweedler (1993). Sweedler's algorithm makes use of a Gröbner basis computation which depends on f. In Kemper (1993) an algorithm is presented which is closely related to Sweedler's results, but the computation of the required Gröbner basis is independent of f. After performing the precomputation, i.e. calculating the Gröbner basis, the answer to Problem 2(B) can be computed efficiently by a kind of reduction of f. The really hard part of Kemper's algorithm is to perform the calculation of the Gröbner basis. Here a "lexicographical block order" (cf. Section 1.4) and tag variables have to be used, i.e. the number of variables required for the computation of the Gröbner basis depends on the number of elements in the given generating set of $\mathbb{K}(\mathbf{g})$. The solutions to Problem 2(A) and 2(B) proposed below make use of a Gröbner basis computation in $\mathbb{K}(\mathbf{x})[\mathbf{Z}]$ independent of f and do not require the use of tag variables or a particular term order.

1.1. INVOLUTION BASES

First we shortly resume Emmy Noether's notion of "involution basis" defined at the beginning of this century which allows a partial solution of Problem 1. The involution form used here also proves useful for determining the degree of separable algebraic extensions (cf. Section 3.1):

Let $g_1, \ldots, g_m \in \mathbb{K}(\mathbf{x})$, $\mathbb{K}(\mathbf{x})$ algebraic of degree d and separable over $\mathbb{K}(\mathbf{g})$. In particular, $x_1, \ldots, x_n$ are algebraic over $\mathbb{K}(\mathbf{g})$. If $u_1, \ldots, u_n$ are transcendental over $\mathbb{K}(\mathbf{g})$ we can define the minimal polynomial $m(Z) \in \mathbb{K}(\mathbf{g}, \mathbf{u})[Z]$ of $\sum_{i=1}^n u_i x_i \in \mathbb{K}(\mathbf{u}, \mathbf{x})$. Over a splitting field $\mathbb{L}$ of $m(Z)$ we have

$$m(Z) = \prod_{i=1}^{d} (Z - \sigma_i(\textstyle\sum_{j=1}^n u_j x_j)) = \prod_{i=1}^{d} (Z - \textstyle\sum_{j=1}^n u_j \sigma_i(x_j))$$

with $\sigma_1, \ldots, \sigma_d \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}(\mathbf{g}, \mathbf{u}))$. Hence $\Phi(\mathbf{u}, Z) := m(Z)$ is a homogeneous polynomial (a form) in $\mathbf{u}, Z$ of degree d. Φ is called the *involution form of* $\mathbb{K}(\mathbf{g})$.

THEOREM 1.1. (NOETHER, 1915, SATZ III) *Let* $g_1, \ldots, g_m \in \mathbb{K}(\mathbf{x})$, $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ *algebraic of degree* d *and separable,* $\Phi(\mathbf{u}, Z)$ *the involution form of* $\mathbb{K}(\mathbf{g})$, $\mathcal{C}(\mathbf{g})$ *the set of coefficients of* $\Phi(\mathbf{u}, Z)$ *excluding elements of* $\mathbb{K}$. *Then*

(i) $\mathcal{C}(\mathbf{g})$ *is finite and uniquely determined by* $\mathbb{K}(\mathbf{g})$*,*
(ii) $\mathbb{K}(\mathcal{C}(\mathbf{g})) = \mathbb{K}(\mathbf{g})$*.*

PROOF. (i) is immediate from the definition.
(ii) As $\Phi(\mathbf{u}, Z)$ is irreducible over $\mathbb{K}(\mathbf{g})$, it is irreducible over $\mathbb{K}(\mathcal{C}(\mathbf{g})) \leq \mathbb{K}(\mathbf{g})$, i.e. $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathcal{C}(\mathbf{g}))] = d$ and $\mathbb{K}(\mathcal{C}(\mathbf{g})) \leq \mathbb{K}(\mathbf{g}) \leq \mathbb{K}(\mathbf{x})$ implies $\mathbb{K}(\mathcal{C}(\mathbf{g})) = \mathbb{K}(\mathbf{g})$.□

For $\mathrm{char}(\mathbb{K}) = 0$, $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ not algebraic, Noether suggests a technique called the "Übertragungsprinzip" which we shall not repeat here. Instead in Section 1.2 an approach to Problem 1 is given which holds in arbitrary characteristic and does not depend on $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ being separable or algebraic. For further details on involution bases we refer to the original work Noether (1915).

For a simple concrete example take the field of rational functions fixed by the cyclic group $C_3 \simeq A_3 = \{\mathrm{id}, (123), (132)\} < S_3$ acting on $\mathbb{Q}(x_1, x_2, x_3)$ by permutation of x_1, x_2, x_3. Here the corresponding involution form immediately computes to

$$\Phi(\mathbf{u}, Z) = (Z-(u_1x_1+u_2x_2+u_3x_3))\cdot(Z-(u_1x_2+u_2x_3+u_3x_1))\cdot(Z-(u_1x_3+u_2x_1+u_3x_2)).$$

In more complicated cases Algorithm 3.2 in Section 3.1 can be applied to compute the involution form.

1.2. CANONICAL BASES BY MEANS OF GRÖBNER BASES

Given $g_1, \ldots, g_m \in \mathbb{K}(\mathbf{x})$, $Z_1, \ldots, Z_n$ indeterminates we can define the ideal

$$\langle Z_1 - x_1, \ldots, Z_n - x_n\rangle \cap \mathbb{K}(\mathbf{g})[\mathbf{Z}].$$

The basic idea is to compute a reduced—and therefore unique—Gröbner basis of this ideal and to use the coefficients hereof as a canonical generating set. Of course this idea requires some elaboration. need

LEMMA 1.2. *Let*

(1) $g_1 = \frac{n_1}{d_1}, \ldots, g_m = \frac{n_m}{d_m} \in \mathbb{K}(\mathbf{x})$*,*
(2) $P := \{p \in \mathbb{K}[\mathbf{x}] : p$ *prime and* $p \mid d_i$ *for some* $i \in \{1, \ldots, m\}\}$*,*
(3) $d := \prod_{p\in P}(p(\mathbf{Z}))^{\eta_p}$ *with* $\eta_p \in \mathbb{N}_{>0}$ *arbitrary,*
(4) $I := \langle n_1(\mathbf{Z}) - g_1 \cdot d_1(\mathbf{Z}), \ldots, n_m(\mathbf{Z}) - g_m \cdot d_m(\mathbf{Z})\rangle \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$*, and*
(5) $J := I : d^\infty \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$*.*

Then for $f \in \mathbb{K}(\mathbf{g})[\mathbf{Z}]$ *the following statements are equivalent:*

(i) $f(Z_1, \ldots, Z_n) \in J$*.*
(ii) $f(x_1, \ldots, x_n) = 0$*.*

In particular, $J \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$ *is prime, and* $J = \langle Z_1 - x_1, \ldots, Z_n - x_n\rangle \cap \mathbb{K}(\mathbf{g})[\mathbf{Z}]$*.*

PROOF. (i)$\Longrightarrow$(ii) Let $f \in J$. Hence there exists a $\mu \in \mathbb{N}_{>0}$ with $d^\mu f \in I$, i.e. there are $q_1, \ldots, q_m \in \mathbb{K}(\mathbf{g})[\mathbf{Z}]$ with

$$d^\mu f = \sum_{i=1}^{m} q_i \cdot (n_i(\mathbf{Z}) - g_i \cdot d_i(\mathbf{Z})),$$

and we have $(d^\mu f)(x_1,\ldots,x_n) = 0$. As $d \in \mathbb{K}[\mathbf{Z}] \setminus \{0\}$ the integrity of $\mathbb{K}(\mathbf{x})$ implies $f(x_1,\ldots,x_n) = 0$.

(ii)$\Longrightarrow$(i) Let $f(Z_1,\ldots,Z_n) \in \mathbb{K}(\mathbf{g})[\mathbf{Z}]$ satisfy (ii). By multiplying f with a suitable $c \in \mathbb{K}[\mathbf{g}]$ we obtain $\tilde{f} = c \cdot f$ with $\tilde{f} \in \mathbb{K}[\mathbf{g}][\mathbf{Z}]$.
It is sufficient to prove

$$\tilde{f} \in \langle n_1(\mathbf{Z}) - g_1 \cdot d_1(\mathbf{Z}),\ldots,n_m(\mathbf{Z}) - g_m \cdot d_m(\mathbf{Z})\rangle : d^\infty \trianglelefteq \mathbb{K}[\mathbf{g}][\mathbf{Z}],$$

because multiplication with c^{-1} then yields $f = c^{-1} \cdot \tilde{f} \in J$. So let

$$\tilde{f} = \sum_{\underline{\mu},\underline{\nu}} \alpha_{\underline{\mu},\underline{\nu}} \cdot \underline{Z}^{\underline{\mu}} \prod_{i=1}^{m} (g_i(\mathbf{x}))^{\nu_i}.$$

Interpreting $\tilde{f}$ as polynomial in $m+n$ variables we have

$$\tilde{f}(g_1(\mathbf{x}),\ldots,g_m(\mathbf{x}),x_1,\ldots,x_n) = 0 = \tilde{f}(g_1(\mathbf{Z}),\ldots,g_m(\mathbf{Z}),Z_1,\ldots,Z_n).$$

Hence

$$\begin{aligned} 0 &= \tilde{f}(g_1(\mathbf{x}) + (g_1(\mathbf{Z}) - g_1(\mathbf{x})),\ldots,g_m(\mathbf{x}) + (g_m(\mathbf{Z}) - g_m(\mathbf{x})),Z_1,\ldots,Z_n) \\ &= \sum_{\underline{\mu},\underline{\nu}} \alpha_{\underline{\mu},\underline{\nu}} \cdot \underline{Z}^{\underline{\mu}} \prod_{i=1}^{m} (g_i(\mathbf{x}) + (g_i(\mathbf{Z}) - g_i(\mathbf{x})))^{\nu_i}. \end{aligned}$$

Expanding the product we obtain only one term not involving a factor of the form $(g_i(\mathbf{Z}) - g_i(\mathbf{x}))$; namely, we have

$$0 = \sum_{\underline{\mu},\underline{\nu}} \alpha_{\underline{\mu},\underline{\nu}} \cdot \underline{Z}^{\underline{\mu}} \left(\prod_{i=1}^{m} (g_i(\mathbf{x}))^{\nu_i} + \sum_{j_{\underline{\nu}}=1}^{m} q_{j_{\underline{\nu}}} \cdot (g_{j_{\underline{\nu}}}(\mathbf{Z}) - g_{j_{\underline{\nu}}}(\mathbf{x})) \right)$$

with $q_{j_{\underline{\nu}}} \in \mathbb{K}[g_1(\mathbf{x}),\ldots,g_m(\mathbf{x}),g_1(\mathbf{Z}),\ldots,g_m(\mathbf{Z}),\mathbf{Z}]$. The last equation can be written as

$$0 = \tilde{f} + \sum_{i=1}^{m} \tilde{q}_i \cdot (g_i(\mathbf{Z}) - g_i(\mathbf{x}))$$

with $\tilde{q}_i \in \mathbb{K}[g_1(\mathbf{x}),\ldots,g_m(\mathbf{x}),g_1(\mathbf{Z}),\ldots,g_m(\mathbf{Z}),\mathbf{Z}]$.
Multiplying with a suitable power product of the $d_i(\mathbf{Z})$ we can remove the denominators of the $g_i(\mathbf{Z})$ and for a suitable $\nu \in \mathbb{N}_{>0}$ we have

$$0 = d^\nu \tilde{f} + \sum_{i=1}^{m} \hat{q}_i \cdot (n_i(\mathbf{Z}) - g_i(\mathbf{x}) d_i(\mathbf{Z}))$$

with $\hat{q}_i \in \mathbb{K}[g_1(\mathbf{x}),\ldots,g_m(\mathbf{x}),\mathbf{Z}]$, i.e.

$$\tilde{f} \in \langle n_1(\mathbf{Z}) - g_1 \cdot d_1(\mathbf{Z}),\ldots,n_m(\mathbf{Z}) - g_m \cdot d_m(\mathbf{Z})\rangle : d^\infty \trianglelefteq \mathbb{K}[\mathbf{g}][\mathbf{Z}]$$

as required.

Using the equivalence (i) $\Longleftrightarrow$ (ii) primality of J is trivial, and it remains to verify $J = \langle Z_1 - x_1,\ldots,Z_n - x_n\rangle \cap \mathbb{K}(\mathbf{g})[\mathbf{Z}]$:

$\subseteq$ From the implication (i)$\Longrightarrow$(ii) we know

$$\forall f \in J : f(Z_1 - (Z_1 - x_1),\ldots,Z_m - (Z_m - x_m)) = 0.$$

Expanding f in the same way as $\tilde{f}$ above the claim follows immediately.

$\supseteq$ A consequence of the implication (ii)$\Longrightarrow$(i). $\square$

For the effective calculation of J we remind the reader of

LEMMA 1.3. *Let I, J, d be as in Lemma 1.2, $d = \prod_{i=1}^{r} q_i$ any factorization of d, and let $Y_1, \ldots, Y_r$ denote new indeterminates.*
Then $J = (I + \langle Y_1 q_1 - 1, \ldots, Y_r q_r - 1\rangle) \cap \mathbb{K}(\mathbf{g})[\mathbf{Z}]$.

PROOF. The proof is a straightforward generalization of the proof of the special case $r = 1$, $q_1 = d$ which can be found in Becker and Weispfenning (1993, Proposition 6.37).

Actually any factorization, including the trivial one, is possible in the above lemma; unfortunately, we do not know of a criteria to decide when using a non-trivial factorization is more efficient than keeping a single polynomial (cf. also the remarks in Section 2.1 of Kemper (1993)).

After having fixed a term order we want to use those coefficients of the reduced Gröbner basis of J which are not contained in $\mathbb{K}$ as a canonical generating set for $\mathbb{K}(\mathbf{g})$ over $\mathbb{K}$—from Lemma 1.2 we know that these coefficients do not depend on the particular generating set of $\mathbb{K}(\mathbf{g})$ chosen. Moreover, as Buchberger's algorithm does not involve operations which require an extension of the ground field we only have to assure that the coefficients of the reduced Gröbner basis are not contained in a proper subfield of $\mathbb{K}(\mathbf{g})$. We prove this by giving an algorithm for expressing arbitrary elements in $\mathbb{K}(\mathbf{g})$ as a rational function in the coefficients of the Gröbner basis.

According to Lemma 1.2 for $\frac{n}{d} \in \mathbb{K}(\mathbf{g})$ the polynomial $n(\mathbf{Z}) - \frac{n}{d} \cdot d(\mathbf{Z})$ is contained in J. So $n(\mathbf{Z}) - \frac{n}{d} d(\mathbf{Z})$ must reduce to zero modulo the Gröbner basis. The key for getting the desired representation in terms of $\mathbf{g}$ is the simple but useful fact given in

REMARK 1.4. Let $p_i \in \mathbb{K}[\mathbf{Z}]$, $A_1, \ldots, A_r$ parameters, $h_i = \frac{n_i}{d_i} \in \mathbb{K}(\mathbf{A}), i = 1, \ldots, s$, G a Gröbner basis of $\langle G\rangle \trianglelefteq \mathbb{K}[\mathbf{Z}]$ w. r. t. an arbitrary term order, $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$ with $\prod_{i=1}^{s} d_i(\alpha_1, \ldots, \alpha_r) \neq 0$.

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

PROOF. As G does not contain elements involving the parameters $\mathbf{A}$ the condition $\prod_{i=1}^{s} d_i(\alpha_1, \ldots, \alpha_r) \neq 0$ also prohibits the denominators occurring successively during the reduction from vanishing. Hence a reduction step after applying the specialization $A_j \mapsto \alpha_j$ either yields a valid reduction step in $\mathbb{K}[\mathbf{Z}]$ or an "empty" reduction, i.e. zero is subtracted. Therefore we obtain a correct reduction of $\sum_{i=1}^{s} h_i(\ \ ) p_i$ when specializing $A_j \mapsto \alpha_j$ after having computed the normal form of $\sum_{i=1}^{s} h_i(\mathbf{A}) p_i$ modulo G.

As specialization does not introduce additional terms further reductions are not possible, i.e. we have reached the normal form of $\sum_{i=1}^{s} h_i(\ \ ) p_i$ modulo G.□

Obviously, choosing $\mathbf{h}$ in Remark 1.4 as linear polynomials in $\mathbf{A}$ causes the resulting normal form to be a polynomial of degree ≤ 1 in $\mathbf{A}$, too.

So, we simply reduce $n(\mathbf{Z}) - A \cdot d(\mathbf{Z})$ modulo the Gröbner basis, thereby reaching a normal form $N(A)$ depending linearly on A. Solving $N(A) = 0$ for A we obtain a rational expression of $\frac{n}{d}$ in terms of the coefficients of the Gröbner basis according to the above remark—note that Lemma 1.2 guarantees the solution f of $N(A) = 0$ to be unique, so the equation cannot be trivial: $n(\mathbf{x}) - f \cdot d(\mathbf{x}) = 0 = n(\mathbf{x}) - \tilde{f} \cdot d(\mathbf{x})$ implies $f = \tilde{f}$.

Next to expressing an element of $\mathbb{K}(\mathbf{g})$ in terms of the coefficients of the Gröbner basis the procedure sketched can be used to decide whether an element $f \in \mathbb{K}(\mathbf{x})$ is contained in $\mathbb{K}(\mathbf{g})$:

LEMMA 1.5. *Let J, $\mathbb{K}(\mathbf{g})$ be as in Lemma 1.2, G a Gröbner basis of J w. r. t. any term order, $n, d \in \mathbb{K}[\mathbf{Z}]$, $d \neq 0$, A a formal parameter, $N(A)$ the normal form of $n - A \cdot d$ modulo G. Then the following statements are equivalent:*

(i) $\frac{n(\mathbf{x})}{d(\mathbf{x})} \in \mathbb{K}(\mathbf{g})$.
(ii) The linear equation $N(A) = 0$ has a solution in $\mathbb{K}(\mathbf{x})$.

PROOF. (i)$\Longrightarrow$(ii) As $\frac{n(\mathbf{x})}{d(\mathbf{x})} \in \mathbb{K}(\mathbf{g})$ we have $n(\mathbf{Z}) - \frac{n(\mathbf{x})}{d(\mathbf{x})} d(\mathbf{Z}) \in J$ according to Lemma 1.2. Thus the claim follows immediately from Remark 1.4.

(ii)$\Longrightarrow$(i) Note that the solution is uniquely determined, as otherwise Remark 1.4 would imply $\forall a \in \mathbb{K}(\mathbf{g}) : n - a \cdot d \in J$ — a contradiction to Lemma 1.2. Moreover, a solution in $\mathbb{K}(\mathbf{x})$ must be a solution in $\mathbb{K}(\mathbf{g})$, because all coefficients involved are contained in $\mathbb{K}(\mathbf{g})$. Thus the claim is an immediate consequence of Lemma 1.2 and Remark 1.4.□

Observe that in the above discussion the assumption that the Gröbner basis is reduced is only required for the uniqueness of the generating set, in particular we have

LEMMA 1.6. *Let J, $\mathbb{K}(\mathbf{g})$ be as in Lemma 1.2, G any Gröbner basis of $J \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$. Then the coefficients of G form a generating set of $\mathbb{K}(\mathbf{g})$ over $\mathbb{K}$.*

After fixing a term order $\preceq$ on $\mathrm{T}(\mathbf{Z})$ an algorithm for finding a canonical generating set now informally consists of two steps:

STEP 1: Compute the reduced Gröbner basis G of $J \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$ w. r. t. $\preceq$.
STEP 2: Extract the coefficients from G.

For practical purposes the computational difficulty lies in the effective execution of the first step, i.e. the calculation of a Gröbner basis in $\mathbb{K}(\mathbf{g})[\mathbf{Z}]$.

1.2.1. COMPUTING A GRÖBNER BASIS IN $\mathbb{K}(\mathbf{g})[\mathbf{Z}]$

The basic problem for the effective computation of a Gröbner basis over $\mathbb{K}(\mathbf{g})$ is the correct treatment of algebraic relations of the generators. One approach for dealing with these "syzygies" is to introduce additional variables for the generators, so-called "tag variables" (cf. Sweedler (1993), Kemper (1993)). As additional variables often increase the cost of the Gröbner basis computation considerably we aim at avoiding this concept. In fact, this is always possible, including the case of $g_1, \ldots, g_m$ being algebraically dependent. We suggest two techniques for accomplishing this:

- Calculating in $\mathbb{K}(\mathbf{x})[\mathbf{Z}]$.
- Introducing "tag parameters" for the generators of a field.

Tag variables still prove useful for determining the algebraic relations of $\{g_1, \ldots, g_m\}$, however. We will make use of this fact in Section 1.4 when replacing explicit computations in $\mathbb{K}(\mathbf{g})$ by computations in a suitable residue class field.

Calculating in $\mathbb{K}(\mathbf{x})[\mathbf{Z}]$: Given polynomials $p_1, \ldots, p_l \in \mathbb{K}(\mathbf{g})[\mathbf{Z}]$ we can clearly calculate a reduced Gröbner basis of $\langle p_1, \ldots, p_l\rangle \trianglelefteq \mathbb{K}(\mathbf{x})[\mathbf{Z}]$. As already mentioned above Buchberger's algorithm does not involve operations requiring an extension of the ground field, thus all computations can be understood as computations in $\mathbb{K}(\mathbf{g})$, i.e. all coefficients are still contained in $\mathbb{K}(\mathbf{g})$, and the result can be interpreted as a Gröbner basis of $\langle p_1, \ldots, p_l\rangle \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$.

If one in interested in expressing the result of an operation explicitly in terms of a given generating set of the field a slightly different approach can be used:

Introducing "tag parameters" for the generators of a field: Treating the generators as formal parameters $g_1, \ldots, g_m$ does not cause any harm as long as we restrict ourselves to addition, subtraction and multiplication, as these operations are defined for all elements in $\mathbb{K}(\mathbf{g})$. Before inverting an element we have to be sure, however, that the according element is not zero. For checking whether an expression is zero we can proceed as above, i.e. we temporarily replace the "tag parameters" $g_1, \ldots, g_m$ by the actual generators $\frac{n_1(\mathbf{x})}{d_1(\mathbf{x})}, \ldots, \frac{n_m(\mathbf{x})}{d_m(\mathbf{x})}$ of $\mathbb{K}(\mathbf{g})$, thereby revealing "hidden syzygies". If the replaced operand does not equal zero in $\mathbb{K}(\mathbf{x})$ the substitution is undone. This kind of "temporary replacement" can be used whenever we have to decide whether an element is zero—although this kind of performing computations in $\mathbb{K}(\mathbf{g})$ seems a bit unwieldy it enables us to avoid the use of tag variables. Moreover, the result of each operation is expressed in terms of the given generators of the field.

Applying this technique to Buchberger's algorithm essentially means to identify the leading coefficients of polynomials, as these are the only elements in $\mathbb{K}(\mathbf{g})$ which have to be inverted: both before calculating S(yzygy)-polynomials and before using polynomials for reduction we determine the "real leading coefficients" of these polynomials by temporarily replacing the tag parameters in the "potential leading coefficients" as described above. If this substitution causes a potential leading coefficient to vanish the remaining polynomial is treated in the same manner. So we finally obtain the zero polynomial or a polynomial with an invertible leading coefficient.

We are now in the position to state

THEOREM 1.7. *Algorithm 1.8 solves the problem of finding a canonical generating set.*

This is immediate from the construction.

Recall that an ideal in a polynomial ring over a field has only finitely many reduced Gröbner bases (cf. Becker and Weispfenning (1993, p. 515)). So one can think of a canonical generating set which is independent of the term order chosen by taking the set of coefficients of all reduced Gröbner bases as a canonical generating set. We do not want to go into details here, however.

ALGORITHM 1.8.

In: $g_1 = \frac{n_1}{d_1}, \ldots, g_m = \frac{n_m}{d_m} \in \mathbb{K}(\mathbf{x})$
$q_1, \ldots, q_r \in \mathbb{K}[\mathbf{Z}]$ *as in Lemma 1.3*
a term order $\leq$ *on* $T(\mathbf{Z})$

Out: $\mathcal{C}$: *a finite canonical generating set of* $\mathbb{K}(\mathbf{g})$ *over* $\mathbb{K}$

begin
Create new indeterminates $Y_1, \ldots, Y_r$.
Select a term order $\preceq$ *on* $\mathrm{T}(Y_1, \ldots, Y_r)$.
$\sqsubseteq \leftarrow$ *the block order satisfying* $\mathbf{Z} \Subset \mathbf{Y}$ *using* $\leq$ *on* $\mathbb{K}[\mathbf{Z}]$ *and* $\preceq$ *on* $\mathbb{K}[\mathbf{Y}]$
$I \leftarrow \bigcup_{i=1}^{m} \{n_i(\mathbf{Z}) - g_i \cdot d_i(\mathbf{Z})\} \cup \bigcup_{j=1}^{r} \{Y_j q_j - 1\}$
$G \leftarrow$ *the reduced Gröbner basis of* $I \cdot \mathbb{K}(\mathbf{x})[\mathbf{Y}, \mathbf{Z}]$ *w. r. t.* $\sqsubseteq$
$G \leftarrow G \cap \mathbb{K}(\mathbf{x})[\mathbf{Z}]$
G contains the reduced Gröbner basis of J (cf. Lemma 1.2) w. r. t. $\leq$.
$\mathcal{C} \leftarrow \left(\bigcup_{g \in G} \{\textit{coefficients of } g\} \right) \setminus \mathbb{K}$
return $\mathcal{C}$
end

Usually, the canonical basis $\mathcal{C}$ computed by Algorithm 1.8 is highly redundant, i.e. one can remove many elements from $\mathcal{C}$ and the remaining set still generates $\mathbb{K}(\mathbf{g})$. Hence it is appropriate to apply some kind of reduction in order to reduce the size of $\mathcal{C}$. As one does not want to give up uniqueness this reduction must be deterministic. Basically one can think of using any kind of strategy here. A natural way of performing the reduction is to select minimal elements from $\mathcal{C}$ after introducing a linear quasi-order $\preceq$ on $\mathbb{K}(\mathbf{g})$. Assuming all elements in $\mathcal{C}$ to be reduced the introduction of a linear quasi-order can be accomplished by using a term order $\leq$ on $\mathrm{T}(D, N, \mathbf{x})$, as any term order $\leq$ on $\mathrm{T}(D, N, \mathbf{x})$ induces a linear quasi-order on $\mathbb{K}[D, N, \mathbf{x}]$ (see Becker and Weispfenning (1993, Theorem 5.12)):

$$\frac{n_1}{d_1} \preceq \frac{n_2}{d_2} \iff N \cdot n_1 + D \cdot d_1 \leq N \cdot n_2 + D \cdot d_2.$$

Using a graded order, i.e. a refinement of the total degree order, and setting

$$\deg\left(\frac{n}{d}\right) := \max(\{\deg(n), \deg(d)\}) \quad (\text{where } \gcd(n, d) = 1)$$

we obtain a quasi-order on $\mathbb{K}(\mathbf{g})$ respecting the total degree of field elements, for example.

1.3. Deciding field membership

To check whether an element of $\mathcal{C}$ is contained in the field generated over $\mathbb{K}$ by a subset of $\mathcal{C}$ already Algorithm 1.10 below, which uses Lemma 1.5 to solve the field membership problem can be applied: if computations in $\mathbb{K}(\mathbf{g})$ are performed by calculating in $\mathbb{K}(\mathbf{x})$ the algorithm solves the non-constructive field membership problem, implementing Algorithm 1.10 by means of "Introducing 'tag parameters' for the generators of a field" as described in Section 1.2.1 enables us to solve the constructive version of Problem 2. Again by construction we have

Theorem 1.9. *Algorithm 1.10 solves the problem of field membership.*

Before looking at a concrete example we give another solution of the constructive field membership problem which enables us to give a characterization of *all* possible representations instead of computing only *one* representation in terms of the generators.

ALGORITHM 1.10. FIELD MEMBERSHIP

In: $g_1 = \frac{n_1}{d_1}, \ldots, g_m = \frac{n_m}{d_m} \in \mathbb{K}(\mathbf{x})$
$q_1, \ldots, q_r \in \mathbb{K}[\mathbf{Z}]$ *as in Lemma 1.3*
a term order $\leq$ *on* $T(\mathbf{Z})$
$f = \frac{n_f}{d_f} \in \mathbb{K}(\mathbf{x})$
Out: h: $h \in \mathbb{K}(\mathbf{g})$ *and* $h =^{\dagger} f$, *if* $f \in \mathbb{K}(\mathbf{g})$,
$h = \perp$, *else*

begin
$G \leftarrow$ *a Gröbner basis of* $J \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$ *as defined in Lemma 1.2 w. r. t.* $\leq$
for a possibility to effectively compute G see Algorithm 1.8
Create a formal parameter A.
$N - A \cdot D \leftarrow$ *the normal form of* $n_f(\mathbf{Z}) - A \cdot d_f(\mathbf{Z})$ *modulo* G
if D=0 # and therefore $N \neq 0$ (see the proof of Lemma 1.5) #
then $h \leftarrow \perp$
else $h \leftarrow \frac{N}{D}$
if $h \notin \mathbb{K}(\mathbf{x})$
then $h \leftarrow \perp$
fi
fi
return h
end

1.4. FINDING ALL REPRESENTATIONS BY MEANS OF TAG VARIABLES

In contrast to Algorithm 1.10 tag variables are used here; the additional variables enable us to express the algebraic relations between the generators. These "syzygies" are the key for characterizing all representations:

LEMMA 1.11. *Let* $f = \frac{n}{d} \in \mathbb{K}(\mathbf{g})$, $h \in \mathbb{K}(T_1, \ldots, T_m)$ *with* $f = h(g_1, \ldots, g_m)$, $S := \{p \in \mathbb{K}[\mathbf{T}] : p(g_1, \ldots, g_m) = 0\}$.
Then for $\tilde{h} \in \mathbb{K}(\mathbf{T})$ *the following statements are equivalent:*

(i) $\tilde{h}(g_1, \ldots, g_m) = f$
(ii) $\exists s \in S, d_T \in \mathbb{K}[\mathbf{T}] \setminus S : \ \tilde{h} = h + \frac{s}{d_T}$

PROOF. (i)$\Longrightarrow$(ii) Let A be a formal parameter, $N(A)$ the normal form of $n - A \cdot d$ modulo G. From Lemma 1.2 and Remark 1.4 we can conclude that both $h(\mathbf{g})$ and $\tilde{h}(\mathbf{g})$ satisfy the non-trivial (see the proof of Lemma 1.5) linear equation $N(A) = 0$. Hence we have $h(\mathbf{g}) - \tilde{h}(\mathbf{g}) = 0$, i.e. the numerator of $h - \tilde{h}$ must be contained in S; the denominator

[†]Note that "=" here denotes equality in $\mathbb{K}(\mathbf{x})$; if tag parameters are used then h contains the representation of f in terms of the generators, i.e. the equality is not syntactical.

of $h - \tilde{h}$ is not contained in S, of course, because neither the denominator of h nor the denominator of $\tilde{h}$ is.

(ii)$\Longrightarrow$(i) Trivial.□

The syzygies (and as will be explained below all representations) can be computed by means of a "tagged version" of Lemma 1.2:

LEMMA 1.12. *Let*

(1) $g_1 = \frac{n_1}{d_1}, \ldots, g_m = \frac{n_m}{d_m} \in \mathbb{K}(\mathbf{x})$,
(2) $P := \{p \in \mathbb{K}[\mathbf{x}] : p \text{ prime and } p \mid d_i \text{ for some } i \in \{1, \ldots, m\}\}$,
(3) $d := \prod_{p \in P} p^{\nu_p}$ *with* $\nu_p \in \mathbb{N}_{>0}$ *arbitrary,*
(4) $T_1, \ldots, T_m$ *new indeterminates ("tag variables"),*
(5) $I_T := \langle n_1 - T_1 \cdot d_1, \ldots, n_m - T_m \cdot d_m \rangle \trianglelefteq \mathbb{K}[\mathbf{T}, \mathbf{x}]$, *and*
(6) $J_T := I_T : d^\infty \trianglelefteq \mathbb{K}[\mathbf{T}, \mathbf{x}]$.

Then for $f \in \mathbb{K}[\mathbf{T}, \mathbf{x}]$ *the following statements are equivalent:*

(i) $f(T_1, \ldots, T_m, \mathbf{x}) \in J_T$.
(ii) $f(g_1, \ldots, g_m, \mathbf{x}) = 0$.

PROOF. The proof is essentially the same as in Lemma 1.2, so we do not go into details here and restrict ourselves on pointing out that for proving (ii)$\Longrightarrow$(i) the expression

$$f(T_1 + (g_1 - T_1), \ldots, T_m + (g_m - T_m), x_1, \ldots, x_n)$$

plays the part of

$$\tilde{f}(g_1(\mathbf{x}) + (g_1(\mathbf{Z}) - g_1(\mathbf{x})), \ldots, g_m(\mathbf{x}) + (g_m(\mathbf{Z}) - g_m(\mathbf{x})), Z_1, \ldots, Z_n)$$

in the proof of Lemma 1.2.□

For effectively calculating J_T we can proceed as in Lemma 1.3:

REMARK 1.13. Let I_T, J_T, d as in Lemma 1.12, $d = \prod_{i=1}^{r} q_i$ any factorization of d, $Y_1, \ldots, Y_r$ new indeterminates.

Then $J_T = (I + \langle Y_1 q_1 - 1, \ldots, Y_r q_r - 1 \rangle) \cap \mathbb{K}[\mathbf{T}, \mathbf{x}]$.

PROOF. As in Lemma 1.3.□

Thus, keeping the notation above, a generating set for J_T can be computed by calculating a Gröbner basis of $\langle n_1 - T_1 \cdot d_1, \ldots, n_m - T_m \cdot d_m, Y_1 \cdot q_1 - 1, \ldots, Y_r \cdot q_r - 1 \rangle$ using any term order satisfying $\mathbf{Y} \gg \mathbf{T}$ and $\mathbf{Y} \gg \mathbf{x}$ followed by removing all polynomials containing any of $\mathbf{Y}$ from the result (see, e.g. Becker and Weispfenning (1993, Proposition 6.15)).

For our purposes we also require $\mathbf{x} \gg \mathbf{T}$, i.e. there are three blocks: $\mathbf{Y} \gg \mathbf{x} \gg \mathbf{T}$

The additional $\mathbf{T}$-block enables us to characterize the syzygies we look for:

REMARK 1.14. Using the above notation and any term order satisfying $\mathbf{Y} \gg \mathbf{x} \gg \mathbf{T}$ let G be a Gröbner basis of $I_T + \langle Y_1 \cdot q_1 - 1, \ldots, Y_r \cdot q_r - 1 \rangle$. Then

(i) $G \cap \mathbb{K}[\mathbf{T}, \mathbf{x}]$ is a Gröbner basis of J_T w. r. t. the induced order,
(ii) $G \cap \mathbb{K}[\mathbf{T}]$ is a Gröbner basis of $S = J_T \cap \mathbb{K}[\mathbf{T}]$ w. r. t. the induced order.

PROOF. (i) follows immediately from Remark 1.13 and what has been said above.
(ii) follows immediately from (i), Lemma 1.12, and the "elimination property" of Gröbner bases (e.g. Becker and Weispfenning (1993, Proposition 6.15)).□

In Kemper (1993) a lexicographical order within the $\mathbf{x}$-block is used, thereby allowing to derive a solution of Problem 2 by means of the given Gröbner basis. For this a "chain of minimal polynomials" is derived from the Gröbner basis (cf. Lemma 2.3).

The algorithm given below uses a different approach. It enables us to solve Problem 2 by means of the given Gröbner basis without having to put any restrictions upon the orders within the blocks.

For deciding field membership it is natural to check for $\frac{n}{d} \in \mathbb{K}(\mathbf{x})$ whether

$$\exists p, q \in \mathbb{K}[\mathbf{T}] : \; n \cdot q - d \cdot p \in J_T \text{ and } q \notin J_T \cap \mathbb{K}[\mathbf{T}], \tag{1.1}$$

i.e. q must not be a syzygy of the generators to keep the denominator from vanishing. If $S = J_T \cap \mathbb{K}[\mathbf{T}]$ as above, $\mathbb{L} :=\text{Quot}(\mathbb{K}[\mathbf{T}]/S)$ denotes the residue class field of $\mathbb{K}[\mathbf{T}]_S$,

$$\pi : \mathbb{K}[\mathbf{T}][\mathbf{x}] \to \mathbb{L}[\mathbf{x}], \; \sum_{\underline{\mu}} a_{\underline{\mu}} \cdot \underline{x}^{\underline{\mu}} \mapsto \sum_{\underline{\mu}} \frac{\overline{a_{\underline{\mu}}}}{\overline{1}} \cdot \underline{x}^{\underline{\mu}}$$

the canonical homomorphism, we can reformulate (1.1) in an obviously equivalent but algorithmically more tractable way:

$$\exists a \in \mathbb{L} : \; \pi(n) - a \cdot \pi(d) \in \langle \pi(J_T) \rangle \trianglelefteq \mathbb{L}[\mathbf{x}].$$

The key for checking this effectively is given by

LEMMA 1.15. *Let G be a Gröbner basis of J_T w. r. t. a term order that satisfies $\mathbf{x} \gg \mathbf{T}$. Then $\pi(G) \setminus \{0\}$ is a Gröbner basis of $\langle \pi(J_T) \rangle \trianglelefteq \mathbb{L}[\mathbf{x}]$ w. r. t. the induced order.*

PROOF. Let $G = \{p_1, \ldots, p_l\}$, $p_i = a_{\underline{\mu}_{i,0}} \underline{x}^{\underline{\mu}_{i,0}} + \sum_{\underline{\mu}_i < \underline{\mu}_{i,0}} a_{\underline{\mu}_i} \underline{x}^{\underline{\mu}_i}$ with $a_{\underline{\mu}_{i,0}}, a_{\underline{\mu}_i} \in \mathbb{K}[\mathbf{T}]$. If $a_{\underline{\mu}_{i,0}} \in S$ and $\underline{\mu}_{i,0} \neq \underline{0}$ for some $i \in \{1, \ldots, l\}$ then

$$\tilde{G} := \{p_i - a_{\underline{\mu}_{i,0}} \underline{x}^{\underline{\mu}_{i,0}}\} \cup (G \setminus \{p_i\})$$

is a Gröbner basis of J_T, too, because both

$$\text{HT}(p_i) = \text{HT}(a_{\underline{\mu}_{i,0}}) \cdot \underline{x}^{\underline{\mu}_{i,0}} \in \langle \text{HT}(\tilde{G}) \rangle \text{ and } \tilde{G} \subseteq J_T$$

according to Remark 1.14 (ii).

W. l. o. g. we can therefore assume $a_{\underline{\mu}_{i,0}} \notin S$ for $i = 1, \ldots, \hat{l}$ and $a_{\underline{\mu}_{i,0}} \in S$ for $i > \hat{l}$. Now let

$$f = b_{\underline{\nu}_0} \cdot \underline{x}^{\underline{\nu}_0} + \sum_{\underline{\nu} < \underline{\nu}_0} b_{\underline{\nu}} \cdot \underline{x}^{\underline{\nu}} \in \langle \pi(J_T) \rangle \trianglelefteq \mathbb{L}[\mathbf{x}], \; b_{\underline{\nu}_0} \neq 0.$$

If $\underline{x}^{\underline{\mu}_{i,0}} \mid \underline{x}^{\underline{\nu}_0}$ for some $i \leq \hat{l}$ then f reduces to $f - \frac{b_{\underline{\nu}_0}}{\pi(a_{\underline{\mu}_{i,0}})} \cdot \underline{x}^{\underline{\nu}_0 - \underline{\mu}_{i,0}}$ modulo $\pi(G) \setminus \{0\}$.

On the other hand, i.e. there is no $i \leq \hat{l}$ satisfying $\underline{x}^{\underline{\mu}_{i,0}} \mid \underline{x}^{\underline{\nu}_0}$, "by clearing denominators in f" we obtain $\tilde{f} \in J_T$, i.e. $\tilde{f}$ must be top-reducible modulo $G \cap \mathbb{K}[\mathbf{T}]$, because G is a Gröbner basis of J_T. If this reduction would "eliminate" $\underline{x}^{\underline{\nu}_0}$ the numerator of $b_{\underline{\nu}_0}$

would be contained in S; a contradiction. But if $\underline{x}^{\underline{\nu}_0}$ would not be "eliminated", we would obtain a polynomial which is not top-reducible modulo $G \setminus \mathbb{K}[\mathbf{T}]$ again. So by induction we had $b_{\underline{\nu}_0} = 0$; a contradiction. Therefore f must be top-reducible modulo $\pi(G) \setminus \{0\}$.□

Using Remark 1.4 an algorithm for solving the problem of constructive field membership now informally can be stated as follows:

STEP 1: Compute a Gröbner basis G of J_T w. r. t. any term order satisfying $\mathbf{x} \gg \mathbf{T}$.
STEP 2: Compute a normal form $\mathrm{N}(A)$ of numerator$(f) - A\cdot$denominator(f) modulo $\pi(G)$.
STEP 3: Check if there is a solution $h \in \mathbb{L}$ of the linear equation $N(A) = 0$, thereby yielding a representation of f.

The effective computation of these steps is rather straightforward:

- Step 1 can be performed by computing a Gröbner basis G as described in Remark 1.14.
- Reading $g \in G$ as a polynomial in $\mathbb{K}[\mathbf{T}][\mathbf{x}]$ we get a Gröbner basis $\pi(G) \subseteq \mathbb{L}[\mathbf{x}]$ of $\langle \pi(J_T) \rangle$ by means of Lemma 1.15. Computing a minimal or reduced Gröbner basis, the default in most computer algebra systems, in Step 1 enables us to identify the leading monomials without further computations (cf. the proof of Lemma 1.15). The computation of the normal forms in Step 2 then consists of calculations in $\mathbb{K}(\mathbf{T})[\mathbf{x}]$ which can be performed by most computer algebra systems.
- To solve the linear equations in Step 3 one is tempted to solve $m \cdot A + b = 0$ in $\mathbb{K}(\mathbf{T}, \mathbf{x})[A]$, i.e. to divide by m. To recognize 0 and remove superfluous terms after cancelling out common factors of the numerator and denominator of m we replace the numerators of m and b by their normal forms modulo $G \cap \mathbb{K}[\mathbf{T}]$, which is a Gröbner basis of S according to Remark 1.14 (ii), before doing so.

A more detailed description of these steps is given in Algorithm 1.17 below, and we can state

THEOREM 1.16. *Algorithm 1.17 solves the problem of constructive field membership.*

Moreover, let $\tilde{S}$ and $\preceq$ be as in Algorithm 1.17. Then $\tilde{S}$ is a Gröbner basis of S w. r. t. $\preceq$ as defined in Lemma 1.11.

PROOF. The theorem follows immediately from the above results; note that the algorithm does not have to handle the case $D = 0 = N$ separately, because in this situation we had $q \cdot d_{f_i} \in J_T$ for some $q \in \mathbb{K}[\mathbf{T}] \setminus S$ and $(q \cdot d_{f_i})(\mathbf{g}, \mathbf{x}) \neq 0$ — in contradiction to Lemma 1.12. □

We remark that the "reduction step" of the algorithm for the field membership problem given in Kemper (1993) in general is more efficient than the one in Algorithm 1.17; as instead of a Gröbner basis a "chain of minimal polynomials" (cf. Lemma 2.3) is used for reduction there, usually less polynomials are involved. The price for this is the necessity of a lexicographical order within the $\mathbf{x}$-block, however.

ALGORITHM 1.17.

In: $g_1 = \frac{n_1}{d_1}, \ldots, g_m = \frac{n_m}{d_m} \in \mathbb{K}(\mathbf{x})$
$q_1, \ldots, q_r \in \mathbb{K}[\mathbf{x}]$ *as in Remark 1.13*
a term order $\leq$ *on* $T(\mathbf{x})$
$f = \frac{n_f}{d_f} \in \mathbb{K}(\mathbf{x})$

Out: $(h, \tilde{S})$: $h \in \mathbb{K}(\mathbf{T})$ *and* $h(\mathbf{g}) = f$, *if* $f \in \mathbb{K}(\mathbf{g})$,
$h = \perp$, *else*
$\tilde{S}$: *a Gröbner basis of* S *as in Remark 1.14 w. r. t.* $\preceq$

begin
Create new indeterminates $T_1, \ldots, T_m, Y_1, \ldots, Y_r$.
Select term orders $\preceq$ *on* $T(\mathbf{T})$ *and* $\preceq'$ *on* $T(\mathbf{Y})$.
$\sqsubseteq \leftarrow$ *the block order satisfying* $\mathbf{T} \Subset \mathbf{x} \Subset \mathbf{Y}$ *using* $\preceq$ *on* $T(\mathbf{T})$, $\leq$ *on* $T(\mathbf{x})$, *and* $\preceq'$ *on* $T(\mathbf{Y})$
$G \leftarrow \bigcup_{i=1}^{m} \{n_i - T_i \cdot d_i\} \cup \bigcup_{j=1}^{r} \{Y_j \cdot q_j - 1\}$
$G \leftarrow$ *a Gröbner basis of* $\langle G \rangle \trianglelefteq \mathbb{K}[\mathbf{T}, \mathbf{x}, \mathbf{Y}]$ *w. r. t.* $\sqsubseteq$
$\tilde{S} \leftarrow G \cap \mathbb{K}[\mathbf{T}]$
$\tilde{G} \leftarrow (G \cap \mathbb{K}[\mathbf{T}, \mathbf{x}]) \setminus \tilde{S}$
Create a formal parameter A.
$N - A \cdot D \leftarrow$ *the normal form of* $n_f - A \cdot d_f$ *modulo* $\tilde{G} \subseteq \mathbb{K}(\mathbf{T})[\mathbf{x}]$
Cancel out common factors of the numerator and denominator of D.
$D \leftarrow \dfrac{\textit{normal form of numerator}(D) \textit{ modulo } \tilde{S}}{\textit{denominator}(D)}$
$N \leftarrow \dfrac{\textit{normal form of numerator}(N) \textit{ modulo } \tilde{S}}{\textit{denominator}(N)}$
if $D=0$
then $h \leftarrow \perp$
else $h \leftarrow \frac{N}{D}$
if $h \notin \mathbb{K}(\mathbf{T})$
then $h \leftarrow \perp$
fi
fi
return $(h, \tilde{S})$
end

1.5. EXAMPLE: THE CANONICAL GENERATING SET OF $\mathbb{Q}(x_1, x_2, x_3)^{A_3}$

The field of invariants $\mathbb{Q}(x_1, x_2, x_3)^{A_3}$ considered in Section 1.1 is given by $\mathbb{Q}(s_1, s_2, s_3, v)$ where

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3, \\ s_2 &= x_1x_2 + x_1x_3 + x_2x_3, \\ s_3 &= x_1x_2x_3, \\ v &= (x_2 - x_1)(x_3 - x_1)(x_3 - x_2). \end{aligned}$$

So the ideal to consider for computing the canonical generating set of $\mathbb{Q}(s_1, s_2, s_3, v)$ is

$$\langle Z_1+Z_2+Z_3-s1, Z_1Z_2+Z_1Z_3+Z_2Z_3-s2, Z_1Z_2Z_3-s3, \\ (Z_2-Z_1)(Z_3-Z_1)(Z_3-Z_2)-v\rangle \trianglelefteq \mathbb{Q}(\mathbf{x})^{A_3}[\mathbf{Z}].$$

Using Algorithm 1.8 with the graded reverse lexicographic order where $Z_1 > Z_2 > Z_3$ we obtain (either by means of tag parameters or by subsequently applying Algorithm 1.17)

$$\left\{ \begin{array}{l} {Z_2}^2 - \frac{1}{2}\frac{2{s_1}^3-7s_1s_2+9s_3-v}{{s_1}^2-3s_2}Z_2 + \frac{v}{{s_1}^2-3s_2}Z_3 + \frac{1}{2}\frac{{s_1}^2s_2-4{s_2}^2+3s_1s_3-s_1v}{{s_1}^2-3s_2}, \\ {Z_3}^2 - \frac{1}{2}\frac{2{s_1}^3-7s_1s_2+9s_3+v}{{s_1}^2-3s_2}Z_3 - \frac{v}{{s_1}^2-3s_2}Z_2 + \frac{1}{2}\frac{{s_1}^2s_2-4{s_2}^2+3s_1s_3+s_1v}{{s_1}^2-3s_2}, \\ Z_2Z_3 - \frac{1}{2}\frac{s_1s_2-9s_3-v}{{s_1}^2-3s_2}Z_2 - \frac{1}{2}\frac{s_1s_2-9s_3+v}{{s_1}^2-3s_2}Z_3 - \frac{3s_1s_3-{s_2}^2}{{s_1}^2-3s_2}, \\ Z_1+Z_2+Z_3-s1 \end{array} \right\}$$

from which the canonical generating set can be read off immediately.

2. Finding the Type of a Field Extension

In this section we give a solution to

PROBLEM 3. *("type of a field extension"): Given $\mathbb{K}(\mathbf{g}) \leq \mathbb{K}(\mathbf{x})$ find the transcendence degree t of $\mathbb{K}(\mathbf{x})$ over $\mathbb{K}(\mathbf{g})$. In case of*

- $(t=0)$ *compute the degree $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]$ and the separability degree $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]_s$; in case of*
- $(t>0)$ *compute a transcendence basis of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ and decide whether this extension is separably generated. In the affirmative case choose the transcendence basis to be separating.*

2.1. ALGEBRAIC AND TRANSCENDENTAL EXTENSIONS

Using Kalkbrener and Sturmfels (1995, Theorem 1) we can compute the dimension of J (which is prime according to Lemma 1.2) by determining the cardinality of any maximal strongly independent subset of $\mathrm{T}(\mathbf{Z})$ modulo J. So if G is a Gröbner basis of J with respect to any term order and X a maximal subset of $\mathrm{T}(\mathbf{Z})$ satisfying $\mathrm{T}(\mathbf{Z}) \cap \mathrm{HT}(G) = \emptyset$ then $\dim(J) = |X|$. The dimension of J is of interest, as we have

LEMMA 2.1. *Let J, $\mathbb{K}(\mathbf{g})$ be as in Lemma 1.2. Then*

(i) $\mathbb{K}(\mathbf{x}) \simeq \mathrm{Quot}(\mathbb{K}(\mathbf{g})[\mathbf{Z}]/J)$, *and*
(ii) the transcendence degree of $\mathbb{K}(\mathbf{x})$ *over* $\mathbb{K}(\mathbf{g})$ *is equal to* $\dim(J)$.

PROOF. The homomorphism defined by

$$\varphi : \mathbb{K}(\mathbf{x}) \to \mathrm{Quot}(\mathbb{K}(\mathbf{g})[\mathbf{Z}]/J), x_i \mapsto \overline{Z_i}/\overline{1}$$

as a homomorphism of fields is trivially injective. As $\mathrm{Quot}(\mathbb{K}(\mathbf{g})[\mathbf{Z}]/J)$ is generated by

$\overline{Z_1}/\overline{1}, \ldots, \overline{Z_n}/\overline{1}, \overline{g_1}/\overline{1}, \ldots, \overline{g_m}/\overline{1}$ over $\mathbb{K}$, the surjectivity follows from

$$\frac{\overline{g_i(\mathbf{x})}}{\overline{1}} = \frac{\overline{n_i(\mathbf{Z}) - (n_i(\mathbf{Z}) - g_i(\mathbf{x})d_i(\mathbf{Z}))}}{\overline{d_i(\mathbf{Z})}} = \frac{\overline{n_i(\mathbf{Z})}}{\overline{d_i(\mathbf{Z})}} = \varphi\left(\frac{n_i(\mathbf{x})}{d_i(\mathbf{x})}\right).$$

As J is prime, every maximally independent set modulo J has $\dim(J)$ elements (Becker and Weispfenning, 1993, Proposition 7.26). So the claim follows from the fact that the residue classes of a maximally independent set modulo a prime ideal $P \trianglelefteq \mathbb{K}[\mathbf{Z}]$ form a transcendence basis of $\mathrm{Quot}(\mathbb{K}[\mathbf{Z}]/P)$ over $\mathbb{K}$ (Becker and Weispfenning, 1993, Lemma 7.25).□

Remember that every strongly independent set modulo an ideal is in particular independent modulo that ideal. So the subset X from above forms a transcendence basis of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ (see the proof of Lemma 2.1), and we can state a partial solution to Problem 3:

Algorithm 2.2.
In: *G: a Gröbner basis of J (cf. Lemma 1.2) w. r. t. an arbitrary term order*
Out: *(t, B): t: the transcendence degree of $\mathbb{K}(\mathbf{x})$ over $\mathbb{K}(\mathbf{g})$*
B: a transcendence basis of $\mathbb{K}(\mathbf{x})$ over $\mathbb{K}(\mathbf{g})$

```
begin
  B ← ∅
  for i ∈ {1, ..., n} do
    if T({Z_j : x_j ∈ B ∪ {x_i}}) ∩ HT(G) = ∅
      then B ← B ∪ {x_i}
    fi
  od
  t ← |B|
  return (t, B)
end
```

Now assume $\dim(J) = 0$, i.e. $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is algebraic. In this case one would like to compute $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]$. Knowing a minimal Gröbner basis G (no $p \in G$ is top-reducible modulo $G \setminus \{p\}$) of J w. r. t. a lexicographic order, e.g. after applying Procedure 4.1 from Faugère *et al.* (1993) in order to convert the given Gröbner basis into a reduced Gröbner basis G w. r. t. a lexicographic order, one can easily derive the required minimal polynomials (cf. Kemper (1993, Theorem 1)):

Lemma 2.3. *Let J, $\mathbb{K}(\mathbf{g})$ be as in Lemma 1.2, G a minimal Gröbner basis of J w. r. t. a lexicographic order such that $Z_1 < \ldots < Z_n$, $i \in \{1, \ldots, n\}$.*
Then selecting $m_i \in G \cap \mathbb{K}(\mathbf{g})[Z_1, \ldots, Z_i]$ of minimal positive degree in Z_i after replacing $Z_1, \ldots, Z_{i-1}$ with $x_1, \ldots, x_{i-1}$ and making the leading coefficient monic, interpreting m_i as polynomial in Z_i, yields the minimal polynomial of x_i over $\mathbb{K}(\mathbf{g})(x_1, \ldots, x_{i-1})$.

Proof. If $m_i(Z_i)$ denotes the minimal polynomial of x_i over $\mathbb{K}(\mathbf{g})(x_1, \ldots, x_{i-1})$, then clearing denominators in $m_i(Z_i)$ by multiplying with a suitable $q \in \mathbb{K}(\mathbf{g})[x_1, \ldots, x_{i-1}]$ after replacing $x_1, \ldots, x_{i-1}$ with $Z_1, \ldots, Z_{i-1}$ yields $\tilde{m}_i(Z_1, \ldots, Z_i) \in \mathbb{K}(\mathbf{g})[Z_1, \ldots, Z_i]$ with $\tilde{m}_i(x_1, \ldots, x_i) = 0$, i.e. $\tilde{m}_i(Z_1, \ldots, Z_i) \in J$ according to Lemma 1.2.

As obviously $q(x_1, \ldots, x_{i-1}) \neq 0$ the leading coefficient of $\tilde{m}_i$, interpreted as a polynomial in Z_i, does not vanish when replacing $Z_1, \ldots, Z_{i-1}$ with $x_1, \ldots, x_{i-1}$. Hence $\tilde{m}_i \notin \langle G \cap \mathbb{K}[Z_1, \ldots, Z_{i-1}] \rangle \trianglelefteq \mathbb{K}(\mathbf{g})[\mathbf{Z}]$, and the reduction of $\tilde{m}_i$ modulo G involves a polynomial of positive degree $\leq \deg(\tilde{m}_i)$ in Z_i. Let $\hat{m}_i$ denote the polynomial in $G \cap \mathbb{K}(\mathbf{g})[Z_1, \ldots, Z_i]$ of minimal positive degree in Z_i.

Requiring G to be minimal prevents the leading coefficient from $\hat{m}_i$, interpreted as a polynomial in Z_i, from vanishing when replacing $Z_1, \ldots, Z_{i-1}$ by $x_1, \ldots, x_{i-1}$, because otherwise the "leading coefficient" would be contained in J thus implying top-reducibility of $\hat{m}_i$ modulo $G \setminus \{\hat{m}_i\}$. So replacing $Z_1, \ldots, Z_{i-1}$ with $x_1, \ldots, x_{i-1}$ in $\hat{m}_i$ yields a non-trivial polynomial in $\mathbb{K}(\mathbf{g})(x_1, \ldots, x_{i-1})[Z_i]$ of degree $\leq \deg(\tilde{m}_i)$ having x_i as a root.

To compute the minimal polynomial of x_i over $\mathbb{K}(\mathbf{g})(x_1, \ldots, x_{i-1})$ we can thus select a polynomial of minimal positive degree in Z_i from $G \cap \mathbb{K}(\mathbf{g})[Z_1, \ldots, Z_i]$. Replacing $Z_1, \ldots, Z_{i-1}$ with $x_1, \ldots, x_{i-1}$ and making the leading coefficient of Z_i monic then yields the desired minimal polynomial.□

Note that if $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is separable the computation of a Gröbner basis w. r. t. a lexicographic order for determining $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]$ is not necessary; in this case it is sufficient to compute (the degree of) the corresponding involution form (cf. Section 1.1) by means of Algorithm 3.2 in Section 3.1. To check whether $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is separable we can, e.g. by means of Algorithm 3.2 from Section 3.1, determine the minimal polynomials $m_1, \ldots, m_n$ of $x_1, \ldots, x_n$ over $\mathbb{K}(\mathbf{g})$. Then the separability of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is equivalent to $\prod_{i=1}^{n} m_i' \neq 0$ where m_i' denotes the formal derivative of m_i (e.g. Bosch (1993, p. 109, Lemma 1)).

In case of $\mathrm{char}(\mathbb{K}) = p > 0$, a "chain of minimal polynomials" as in Lemma 2.3 can be used to compute the degree of separability $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]_s$: Let $m_i(Z)$ be the minimal polynomial of x_i over $\mathbb{K}(\mathbf{g})(x_1, \ldots, x_{i-1})$, $r_i \in \mathbb{N}_{\geq 0}$ maximal with $m_i = \tilde{m}_i(Z^{p^{r_i}})$ for some $\tilde{m}_i(Z) \in \mathbb{K}[Z]$, $i = 1, \ldots, n$. Then $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]_s$ equals $\prod_{i=1}^{n}(\deg(m_i)/p^{r_i})$ (e.g. Bosch (1993, p. 111, Lemma 6)).

Hence for $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ algebraic the problem of finding the type of a field extension can essentially be reduced to the computation of a minimal Gröbner basis of J w. r. t. a lexicographic term order.

If $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is not algebraic, then a separating transcendence basis, in case of existence, can be selected from $2^{\{x_1, \ldots, x_n\}}$ (e.g. Winter (1974, Theorem 4.3.11)). So after computing the transcendence degree t of $\mathbb{K}(\mathbf{x})$ over $\mathbb{K}(\mathbf{g})$ we can proceed as in the algebraic case to check for all $\binom{n}{t}$ subsets $X \subseteq \{x_1, \ldots, x_n\}$ having t elements, whether $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})(X)$ is a separable algebraic extension, thereby obtaining a separating transcendence basis if and only if $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is separably generated, of course an exhaustive search like this is practical for small values of t only.

Combining the results in this section in the obious way we obtain a complete solution to the problem of finding the type of a field extension. As the implementation of the individual steps is straightforward we omit giving an explicit algorithm, and restrict ourselves to stating

THEOREM 2.4. *The problem of finding the type of a field extension can be solved effectively.*

2.2. example: a representation of $\mathbb{Z}/6\mathbb{Z}$ over $\mathbb{F}_5$

The mapping

$$\mathbb{Z}/6\mathbb{Z} \to \mathrm{GL}(3,\mathbb{F}_5), 1 \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 4 & 0 & 0 \end{pmatrix}$$

defines a three dimensional representation of the cylic group with six elements over $\mathbb{F}_5$. The corresponding field of invariants $\mathbb{F}_5(x,y,z)^{\mathbb{Z}/6\mathbb{Z}}$ over $\mathbb{F}_5$ is generated by

$$\{\, x^2+y^2+z^2, xy+4xz+yz, x^4+y^4+z^4, x^3y+4xz^3+y^3z,$$
$$x^6+y^6+z^6, x^5y+4xz^5+y^5z \,\}.$$

In order to find the type of the extension $\mathbb{F}_5(x,y,z)/\mathbb{F}_5(x,y,z)^{\mathbb{Z}/6\mathbb{Z}}$ we consider the ideal

$$\langle X^2+Y^2+Z^2+4(x^2+y^2+z^2), XY+4XZ+YZ+4(xy+4xz+yz),$$
$$X^4+Y^4+Z^4+4(x^4+y^4+z^4), X^3Y+4XZ^3+Y^3Z+4(x^3y+4xz^3+y^3z),$$
$$X^6+Y^6+Z^6+4(x^6+y^6+z^6),$$
$$X^5Y+4XZ^5+Y^5Z+4(x^5y+4xz^5+y^5z)\rangle \trianglelefteq \mathbb{F}_5(x,y,z)^{\mathbb{Z}/6\mathbb{Z}}[X,Y,Z].$$

As in Section 1.5 the saturation can be omitted here, as the generators are polynomials. Using the lexicographical term order with $X > Y > Z$ we obtain the following reduced Gröbner basis:

$$\Big\{ X + \frac{4x^4y+4x^3z^2+x^2y^3+xz^4+y^4z+4y^2z^3}{x^5y^3z+4x^5yz^3+4x^3y^5z+x^3yz^5+xy^5z^3+4xy^3z^5} Z^5$$
$$+ \frac{x^6y+x^5z^2+4x^2y^5+4xz^6+4y^6z+y^2z^5}{x^5y^3z+4x^5yz^3+4x^3y^5z+x^3yz^5+xy^5z^3+4xy^3z^5} Z^3$$
$$+ \frac{4x^6y^3+4x^5z^4+x^4y^5+x^3z^6+y^6z^3+4y^4z^5}{x^5y^3z+4x^5yz^3+4x^3y^5z+x^3yz^5+xy^5z^3+4xy^3z^5} Z,$$
$$Y + \frac{x^4z+4x^3y^2+4x^2z^3+xy^4+y^3z^2+4yz^4}{x^5y^3z+4x^5yz^3+4x^3y^5z+x^3yz^5+xy^5z^3+4xy^3z^5} Z^5$$
$$+ \frac{4x^6z+x^5y^2+x^2z^5+4xy^6+4y^5z^2+yz^6}{x^5y^3z+4x^5yz^3+4x^3y^5z+x^3yz^5+xy^5z^3+4xy^3z^5} Z^3$$
$$+ \frac{x^6z^3+4x^5y^4+4x^4z^5+x^3y^6+y^5z^4+4y^3z^6}{x^5y^3z+4x^5yz^3+4x^3y^5z+x^3yz^5+xy^5z^3+4xy^3z^5} Z,$$
$$Z^6 + (4x^2+4y^2+4z^2)Z^4 + (x^2y^2+x^2z^2+y^2z^2)Z^2 + 4x^2y^2z^2 \Big\}$$

From this we immediately recognize $\mathbb{F}_5(x,y,z)/\mathbb{F}_5(x,y,z)^{Z/6Z}$ as a separable algebraic extension of degree 6.

3. Computing Minimal Polynomials and Finding Special Elements

3.1. computing minimal polynomials

As for $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ algebraic and separable the degree of the involution form is equal to $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]$ (cf. Section 1.1), we can compute the degree of a separable algebraic extension by solving

PROBLEM 4. *("finding minimal polynomials"):*
Given $\mathbb{K}(\mathbf{g}) \leq \mathbb{K}(\mathbf{x})$ *and* $f \in \mathbb{K}(\mathbf{x})$ *algebraic over* $\mathbb{K}(\mathbf{g})$ *compute the minimal polynomial of* f *over* $\mathbb{K}(\mathbf{g})$.

If $f = \frac{n}{d} \in \mathbb{K}(\mathbf{x})$ is algebraic over $\mathbb{K}(\mathbf{g})$ with minimal polynomial

$$m_f(Z) = Z^l + \sum_{i=0}^{l-1} \alpha_i Z^i,\ \alpha_i \in \mathbb{K}(\mathbf{g})$$

and G a Gröbner basis of J as in Lemma 1.2 then the normal form of

$$\tilde{f}_l(\ \ ,\mathbf{Z}) := (d(\mathbf{Z}))^l \left((f(\mathbf{Z}))^l + \sum_{i=0}^{l-1} \alpha_i \cdot (f(\mathbf{Z}))^i \right)$$

modulo G is zero, because $\tilde{f}_l(\ \ ,\mathbf{Z}) \in J$ according to Lemma 1.2.

If on the other hand $\tilde{f}_l(\ \ ,\mathbf{Z})$ reduces to zero modulo G for some $\alpha_0, \ldots, \alpha_{l-1} \in \mathbb{K}(\mathbf{g})$ then clearly $f(\mathbf{x})^l + \sum_{i=0}^{l-1} \alpha_i \cdot (f(\mathbf{x}))^i = 0$.

By considering Remark 1.4 we can find the minimal polynomial of f by checking successively for $l = 1, 2, \ldots$[†] whether the normal form of $\tilde{f}_l(\ \ ,\mathbf{Z})$ modulo G vanishes for some $\ \ \in \mathbb{K}(\mathbf{g})$. This can be checked efficiently by solving the linear equation system we get when equating all coefficients in the normal form of

$$(d(\mathbf{Z}))^l \left((f(\mathbf{Z}))^l + \sum_{i=0}^{l-1} A_i \cdot (f(\mathbf{Z}))^i \right)$$

to zero [‡], $\mathbf{A}$ formal parameters. As we check small values of l first the uniqueness of the minimal polynomial guarantees that the solution of the first solvable linear equation system is unique. Furthermore, as all of the coefficients involved are contained in $\mathbb{K}(\mathbf{g})$, it is sufficient to look for solutions in $\mathbb{K}(\mathbf{x})$, of course.

We are now in the position to state an effective algorithm for solving Problem 4, and by construction we have

THEOREM 3.1. *Algorithm 3.2 solves the problem of finding minimal polynomials.*

ALGORITHM 3.2.

In: *G: a Gröbner basis of J (cf. Lemma 1.2) w. r. t. an arbitrary term order*
$f = \frac{n_f}{d_f} \in \mathbb{K}(\mathbf{x})$ *algebraic over* $\mathbb{K}(\mathbf{g})$
Out: *p: the minimal polynomial of* f *over* $\mathbb{K}(\mathbf{g})$

begin
Create a new indeterminate Z.

[†]If $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is algebraic of known degree it is sufficient to consider the divisors of $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})]$, of course.

[‡]One could be tempted to conclude from J being prime and $d(\mathbf{x}) \neq 0$ that it is sufficient to consider the normal form of $(f(\mathbf{Z}))^l + \sum_{i=0}^{l-1} A_i \cdot (f(\mathbf{Z}))^i$. However, the latter in general is a rational function, i.e. the factor $d(\mathbf{Z})^l$ is needed for clearing denominators.

$l \leftarrow 1$
repeat
Create a formal parameter A_{l-1}.
$\tilde{f} \leftarrow (d_f(\mathbf{Z}))^l \left((f(\mathbf{Z}))^l + \sum_{j=0}^{l-1} A_j \cdot (f(\mathbf{Z}))^j \right)$
$\sum_{\underline{\mu}} a_{\underline{\mu}}(A_0, \ldots, A_{l-1}) \cdot \underline{Z}^{\underline{\mu}} \leftarrow$ *the normal form of* $\tilde{f}$ *modulo* G
$A \leftarrow \{(\alpha_0, \ldots, \alpha_{l-1}) \in \mathbb{K}(\mathbf{x}) | \forall \underline{\mu} : a_{\underline{\mu}}(\alpha_0, \ldots, \alpha_{l-1}) = 0\}$
if $A \neq \emptyset$
then select $(\alpha_0, \ldots, \alpha_{l-1}) \in A$
$p \leftarrow Z^l + \sum_{j=0}^{l-1} \alpha_j Z^j$
fi
$l \leftarrow l + 1$
until $A \neq \emptyset$
return p
end

Note that Algorithm 3.2 as stated above does not decide whether an element f is algebraic over $\mathbb{K}(\mathbf{g})$. For this an upper bound for the degree of the minimal polynomial of f has to be known.

One (somewhat unpleasant) possibility is to determine a transcendence basis of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ as described in Algorithm 2.2; if a transcendence basis is known an upper bound can be derived by applying the techniques for computing the degree of an algebraic extension to

REMARK 3.3. Let $f \in \mathbb{K}(\mathbf{x})$ be algebraic over $\mathbb{K}(\mathbf{g})$, B a transcendence basis of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$. Then $[\mathbb{K}(\mathbf{g})(f) : \mathbb{K}(\mathbf{g})] \leq [\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})(B)]$.

PROOF. As the minimal polynomials of f over $\mathbb{K}(\mathbf{g})$ and $\mathbb{K}(\mathbf{g})(B)$ coincide we have $[\mathbb{K}(\mathbf{g})(f) : \mathbb{K}(\mathbf{g})] = [\mathbb{K}(\mathbf{g})(B)(f) : \mathbb{K}(\mathbf{g})(B)] \leq [\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})(B)]$.□

A simpler way for calculating the required upper bound is given in

LEMMA 3.4. *If* $f \in \mathbb{K}(\mathbf{x})$ *is algebraic over* $\mathbb{K}(\mathbf{g})$ *then* $[\mathbb{K}(\mathbf{g})(f) : \mathbb{K}(\mathbf{g})] \leq \prod_{i=1}^{m} \deg(g_i)$.

PROOF. Let $B \subseteq \{\mathbf{x}\}$ be a transcendence basis of $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$, H a maximal (over $\mathbb{K}$) algebraically independent subset of $\{\mathbf{g}\}$, $\tilde{B} := B \cup H$.

It is sufficient to prove

$$[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\tilde{B})] \leq \prod_{g \in \tilde{B}} \deg(g),$$

because using Remark 3.3 we then have

$$[\mathbb{K}(\mathbf{g})(f) : \mathbb{K}(\mathbf{g})] \leq [\mathbb{K}(\mathbf{x}) : \mathbb{K}(\mathbf{g})(B)] \leq [\mathbb{K}(\mathbf{x}) : \mathbb{K}(\tilde{B})] \leq \prod_{g \in \tilde{B}} \deg(g) \leq \prod_{i=1}^{m} \deg(g_i).$$

Using a new transcendental element x_0 we can define the $\mathbb{K}$-isomorphism

$$\varphi : \mathbb{K}(\mathbf{x}) \to \mathbb{K}\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right), \; x_i \mapsto \frac{x_i}{x_0}.$$

Obviously $\varphi(\tilde{B})$ is algebraically independent over $\mathbb{K}$, so by means of the estimation from Lemma 3.10 (b) in Kemper (1994) we obtain

$$[\mathbb{K}(x_1/x_0, \ldots, x_n/x_0) : \mathbb{K}(\{\varphi(g) : g \in \tilde{B}\})] \leq \prod_{g \in \tilde{B}} \deg(\varphi(g)).$$

As $\deg(g) = \deg(\varphi(g))$ for $g \in \tilde{B}$ we have $[\mathbb{K}(\mathbf{x}) : \mathbb{K}(\tilde{B})] \leq \prod_{g \in \tilde{B}} \deg(g)$.□

We can now solve

Problem 5. *("recognizing algebraic elements"):*
Given $\mathbb{K}(\mathbf{g}) \leq \mathbb{K}(\mathbf{x})$ *and* $f \in \mathbb{K}(\mathbf{x})$ *decide whether* f *is algebraic or transcendental over* $\mathbb{K}(\mathbf{g})$.

As the modifications of Algorithm 3.2 are straightforward we forego stating an explicit algorithm for solving Problem 5. We have

Theorem 3.5. *The problem of recognizing algebraic elements can be solved effectively by combining Algorithm 3.2 with Lemma 3.4.*

Proof. The claim is an immediate consequence of the above results.□

3.2. finding special elements

The technique used for computing minimal polynomials yields an obvious algorithm for finding arbitrary polynomials of degree $\leq l \in \mathbb{N}_{\geq 0}$ in $\mathbb{K}(\mathbf{g})$; we simply have to look at the normal form of $\sum_{1 \leq |\underline{\mu}| \leq l} A_{\underline{\mu}} \cdot (\underline{Z}^{\underline{\mu}} - \underline{x}^{\underline{\mu}})$ modulo G which yields a system of linear equations over $\mathbb{K}$. By specializing some of the $A_{\underline{\mu}}$ in advance we can force a "particular structure" of the polynomial.

Finding polynomials is of interest if $\mathbb{K}(\mathbf{g})$ is known to have a polynomial generating set, for instance:

Lemma 3.6. *Let* $\mathbf{g} \in \mathbb{K}[\mathbf{x}], \mathbb{K}(\mathbf{g})(r_1, \ldots, r_v)$ *be an intermediate field of* $\mathbb{K}(\mathbf{g})$ *and* $\mathbb{K}(\mathbf{x})$ *with* $\mathbb{K}(\mathbf{g})(\mathbf{r})/\mathbb{K}(\mathbf{g})$ *algebraic.*
Then there are $h_1, \ldots, h_r \in \mathbb{K}[\mathbf{x}] : \mathbb{K}(\mathbf{g})(\mathbf{r}) = \mathbb{K}(\mathbf{g})(\mathbf{h})$.

Proof. Using induction we can assume $v = 1$. Let $r_1 = \frac{n}{d}, \gcd(n, d) = 1, m \in \mathbb{K}(\mathbf{g})[Z]$ the minimal polynomial of ${r_1}^{-1} = \frac{d}{n}$ over $\mathbb{K}(\mathbf{g})$, and select $p_0, \ldots, p_l, q \in \mathbb{K}[\mathbf{Z}]$ such that $m(Z) = (\sum_{i=0}^{l} p_i(\mathbf{g}) \cdot Z^i)/q(\mathbf{g})$. Clearing denominators in the equation $m(\frac{d}{n}) = 0$ and subtracting $p_0(\mathbf{g}) \cdot n^l$ on both sides we obtain $-p_0(\mathbf{g}) \cdot n^l = d \cdot \sum_{i=1}^{l} p_i(\mathbf{g}) \cdot d^{i-1} n^{l-i}$, i.e. d is a divisor of $p_0(\mathbf{g})$. As clearly $p_0(\mathbf{g}) \neq 0$ the claim is a consequence of the equality $\mathbb{K}(\mathbf{g})(\frac{n}{d}) = \mathbb{K}(\mathbf{g})(n \cdot \frac{p_0(\mathbf{g})}{d})$.□

Finding polynomials can be regarded as a special variant of the more general

PROBLEM 6. *("special elements"):*
Given parameters $A_1, \ldots, A_v$, $f(\mathbf{A}, \mathbf{x}) \in \mathbb{K}(\mathbf{A}, \mathbf{x})$, *and* $\mathbb{K}(\mathbf{g}) \leq \mathbb{K}(\mathbf{x})$ *where* $\mathbb{K}$ *is algebraically closed decide if there is a specialization* $(\mathbf{A}) \mapsto (\alpha_1, \ldots, \alpha_v)$ *with* $\in \mathbb{K}$ *such that* $f(\ , \mathbf{x}) \in \mathbb{K}(\mathbf{g})$.

An algorithm for solving this problem which also computes possible values of $\mathbf{A}$ can be used to look for elements of minimal positive degree in $\mathbb{K}(\mathbf{g})$, for example, by checking successively whether there are elements of degree 1,2,... in $\mathbb{K}(\mathbf{g})$.

Keeping the above notation an answer to Problem 6 can be sketched as follows:

STEP 1: Compute the normal form $N(f) := \frac{n_N(\mathbf{A},\mathbf{x},\mathbf{Z})}{d_N(\mathbf{A},\mathbf{x})}$ of $n_f(\mathbf{A}, \mathbf{Z}) - f(\mathbf{A}, \mathbf{x}) \cdot d_f(\mathbf{A}, \mathbf{Z})$ modulo G; let I_n resp. I_d denote the ideal corresponding to the (polynomial) equation system we obtain when equating the coefficients in $n_N(\mathbf{A}, \mathbf{x}, \mathbf{Z}) \in \mathbb{K}[\mathbf{A}][\mathbf{x}, \mathbf{Z}]$ resp. $d_f(\mathbf{A}, \mathbf{x}) \in \mathbb{K}[\mathbf{A}][\mathbf{x}]$ to zero.
STEP 2: Check if $\mathrm{V}(I_n) \subseteq \mathrm{V}(I_d)$, i.e. $\mathrm{V}(I_n) \setminus \mathrm{V}(I_d) = \emptyset$.

For performing the second step effectively we can check whether $\sqrt{I_n} \supseteq I_d$ by means of a radical membership test as described in Becker and Weispfenning (1993, p. 268), for example. If $I_d \not\subseteq \sqrt{I_n}$ the possible values of $\mathbf{A}$ are given by $\mathrm{V}(I_n) \setminus \mathrm{V}(I_d)$, of course. As the implementation of the individual steps is straightforward we skip the details and state

THEOREM 3.7. *The problem of special elements can be solved effectively.*

PROOF. The claim is an immediate consequence of Remark 1.4 and the above.□

Note that for satisfying a particular structure it can be necessary to use a non-reduced representation of an element, as a trivial example think of $\frac{{x_1}^3}{A_1 \cdot x_1 + A_1 - 1}$ and $\mathbb{C}({x_1}^2)$ where $A_1 \mapsto 1$ is the only specialization possible.

3.3. EXAMPLE: THE INVOLUTION FORM OF $\mathbb{R}(x_1x_2, x_1 + x_2)$

To give a simple concrete example for the practical calculation of a minimal polynomial we can compute the involution form (cf. Section 1.1) of $\mathbb{R}(x_1x_2, x_1+x_2)$, i.e. the minimal polynomial of $u_1x_1 + u_2x_2$ over $\mathbb{R}(u_1, u_2)(x_1x_2, x_1 + x_2)$. The ideal to consider is

$$\langle Z_1Z_2 - x_1x_2, Z_1 + Z_2 - (x_1 + x_2)\rangle \trianglelefteq \mathbb{R}(u_1, u_2, x_1, x_2)[Z_1, Z_2].$$

Using the lexicographic term order with $Z_1 > Z_2$ we obtain the reduced Gröbner basis

$$G := \{Z_1 + Z_2 - (x_1 + x_2), {Z_2}^2 - (x_1 + x_2) \cdot Z_2 + x_1x_2\}.$$

Following Algorithm 3.2 we first have to compute the normal form of $(u_1 \cdot Z_1 + u_2 \cdot Z_2) + A_0$ modulo G with a formal parameter A_0. The normal form computes to

$$(u_2 - u_1) \cdot Z_2 + (x_1 + x_2)u_1 + A_0$$

and does not vanish for any specialization $A_0 \mapsto \alpha_0$, $\alpha_0 \in \mathbb{R}(x_1, x_2, u_1, u_2)$. Therefore the normal form of $(u_1 \cdot Z_1 + u_2 \cdot Z_2)^2 + A_1 \cdot (u_1 \cdot Z_1 + u_2 \cdot Z_2) + A_0$ modulo G has to be computed with A_1 denoting a formal parameter:

$$((u_2 - u_1)A_1 + (x_1 + x_2)({u_2}^2 - {u_1}^2))Z_2 + (x_1 + x_2)u_1A_1 + A_0 - x_1x_2(u_1 - u_2)^2 + (x_1 + x_2)^2{u_1}^2.$$

A simple calculation shows that the latter vanishes under the specialization

$$(A_0, A_1) \mapsto (x_1x_2(u_1 - u_2)^2 + (x_1 + x_2)^2u_1u_2, -(x_1 + x_2)(u_1 + u_2)),$$

i.e. the required minimal polynomial is

$$Z^2 - (x_1 + x_2)(u_1 + u_2) \cdot Z + x_1x_2(u_1 - u_2)^2 + (x_1 + x_2)^2u_1u_2.$$

4. Intermediate Fields

4.1. intermediate fields and primary decomposition

One motivation for looking at subfields of $\mathbb{K}(\mathbf{x})$ is multivariate rational decomposition: When decomposing univariate rational functions subfields of $\mathbb{K}(x)$ are of interest (cf. Zippel (1991)); so it seems natural to look at subfields of $\mathbb{K}(\mathbf{x})$ when trying to generalize these techniques. Given a minimal primary decomposition of $J \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$, i.e. the ideal generated in $\mathbb{K}(\mathbf{x})[\mathbf{Z}]$ by the elements of J $(= J \cdot \mathbb{K}(\mathbf{g})[\mathbf{Z}])$, we can derive information about the intermediate fields of $\mathbb{K}(\mathbf{g})$ and $\mathbb{K}(\mathbf{x})$. In order to be able to make this more precise we remind the reader of

Lemma 4.1. *Let $\mathbb{L}/\mathbb{K}$ denote a (not necessarily algebraic) separable extension of fields, $I \trianglelefteq \mathbb{K}[Z_1, \ldots, Z_n]$ a radical ideal. Then the following statements hold:*

(i) $I \cdot \mathbb{L}[\mathbf{Z}]$ is radical.
(ii) If $\mathbb{K}$ is algebraically closed in $\mathbb{L}$ and I is prime then $I \cdot \mathbb{L}[\mathbf{Z}]$ is prime.

Proof. (i) A consequence of (Eisenbud, 1995, Exercise A1.1)
(ii) A consequence of (Eisenbud, 1995, Exercise A1.2 a)□

By means of this lemma we can derive

Lemma 4.2. *Let*

(1) $J = J \cdot \mathbb{K}(\mathbf{g})[\mathbf{Z}]$, $\mathbb{K}(\mathbf{g})$ as in Lemma 1.2,
(2) $J \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}] = \bigcap_{i=1}^{l} Q_i$ a minimal primary decomposition,
(3) P_i the associated prime of Q_i, $i = 1, \ldots, l$,
(4) $\mathbb{L}$ an intermediate field of $\mathbb{K}(\mathbf{g})$ and $\mathbb{K}(\mathbf{x})$,
(5) $\mathbb{K}(\mathbf{g})_{\text{alg}}$ the algebraic closure of $\mathbb{K}(\mathbf{g})$ in $\mathbb{K}(\mathbf{x})$.

Then for $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ algebraic the following statements hold:

(i) If $\mathbb{K}(\mathbf{x})/\mathbb{L}$ is separable then there is $\Lambda \subseteq \{1, \ldots, l\}$: After removing the elements of $\mathbb{K}$ the coefficients of a reduced Gröbner basis of $\bigcap_{\lambda \in \Lambda} P_\lambda$ form the canonical generating set of $\mathbb{L}$ as computed by Algorithm 1.8.
(ii) If $\mathbb{L}/\mathbb{K}(\mathbf{g})$ is separable then there is $\Lambda \subseteq \{1, \ldots, l\}$: After removing the elements of $\mathbb{K}$ the coefficients of a reduced Gröbner basis of $\bigcap_{\lambda \in \Lambda} Q_\lambda$ form the canonical generating set of $\mathbb{L}$ as computed by Algorithm 1.8.
(iii) Up to permutation $Q_1, \ldots, Q_l$ are uniquely determined.
(iv) If $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is separable $\forall i = 1, \ldots, l : \ Q_i = P_i$.

For $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})_{\mathrm{alg}}$ separable (not necessarily algebraic) there is a $\lambda \in \{1,\ldots,l\}$: After removing the elements of $\mathbb{K}$ the coefficients of a reduced Gröbner basis of P_λ form the canonical generating set of $\mathbb{K}(\mathbf{g})_{\mathrm{alg}}$ as computed by Algorithm 1.8.

Proof. We first prove the statements for the algebraic case; hence until stated otherwise $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is assumed to be algebraic. We can split the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ into the steps $\mathbb{K}(\mathbf{g}) \subseteq \mathbb{K}(\mathbf{g})_{\mathrm{sep}} \subseteq \mathbb{K}(\mathbf{x})$ where $\mathbb{K}(\mathbf{g})_{\mathrm{sep}}/\mathbb{K}(\mathbf{g})$ is separable and $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})_{\mathrm{sep}}$ is purely inseparable.

Now assume $\mathbb{L}/\mathbb{K}(\mathbf{g})$ to be separable. From Lemma 4.1 (i) we conclude that $J \cdot \mathbb{L}[\mathbf{Z}]$ is radical and of dimension zero. In particular, its primary components are the prime ideals it is contained in. Note that if $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ is separable we obtain (iv) by applying the latter argumentation to $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$.

Let $J_\mathbb{L} = J_\mathbb{L} \cdot \mathbb{L}[\mathbf{Z}]$ denote the prime ideal corresponding to $\mathbb{L}$ according to Lemma 1.2. In particular, $J_\mathbb{L}$ is prime. Moreover, we clearly have $J \cdot \mathbb{L}[\mathbf{Z}] \subseteq J_\mathbb{L} \cdot \mathbb{L}[\mathbf{Z}]$, i.e. $J_\mathbb{L} \cdot \mathbb{L}[\mathbf{Z}]$ is a primary component/an associated prime of $J \cdot \mathbb{L}[\mathbf{Z}]$, and we have a primary decomposition of the form

$$J \cdot \mathbb{L}[\mathbf{Z}] = J_\mathbb{L} \cdot \mathbb{L}[\mathbf{Z}] \cap \bigcap_{i=1}^{l'} P_{\mathbb{L},i}$$

where $P_{\mathbb{L},1},\ldots,P_{\mathbb{L},l'} \trianglelefteq \mathbb{L}[\mathbf{Z}]$ are prime.

As above we recognize $J_\mathbb{L} \cdot \mathbb{K}(\mathbf{g})_{\mathrm{sep}}[\mathbf{Z}], P_{\mathbb{L},1} \cdot \mathbb{K}(\mathbf{g})_{\mathrm{sep}}[\mathbf{Z}],\ldots,P_{\mathbb{L},l'} \cdot \mathbb{K}(\mathbf{g})_{\mathrm{sep}}[\mathbf{Z}]$ as radical. As all of these ideals are of dimension zero their associated primes cannot properly contain each other, and we have a primary decomposition of the form

$$J \cdot \mathbb{K}(\mathbf{g})_{\mathrm{sep}}[\mathbf{Z}] = \bigcap_{i=1}^{l''} P_{\mathbb{K}(\mathbf{g})_{\mathrm{sep}},i} \cap \bigcap_{i=l''+1}^{l'''} P_{\mathbb{K}(\mathbf{g})_{\mathrm{sep}},i}$$

with $P_{\mathbb{K}(\mathbf{g})_{\mathrm{sep}},1},\ldots,P_{\mathbb{K}(\mathbf{g})_{\mathrm{sep}},l'''} \trianglelefteq \mathbb{K}(\mathbf{g})_{\mathrm{sep}}[\mathbf{Z}]$ prime and $J_\mathbb{L} \cdot \mathbb{K}(\mathbf{g})_{\mathrm{sep}}[\mathbf{Z}] = \bigcap_{i=1}^{l''} P_{\mathbb{K}(\mathbf{g})_{\mathrm{sep}},i}$.

Now let $i \in \{1,\ldots,l'''\}$, $\tilde{Q}_i := P_{\mathbb{K}(\mathbf{g})_{\mathrm{sep}},i}$, $p,q \in \mathbb{K}(\mathbf{x})[\mathbf{Z}]$ such that $p \cdot q \in \tilde{Q}_i \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$. From $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})_{\mathrm{sep}}$ being purely inseparable we know that there is $e \in \mathbb{N}_{>0}$ such that $p^e, q^e \in \mathbb{K}(\mathbf{g})_{\mathrm{sep}}[\mathbf{Z}]$ and $p^e q^e \in \tilde{Q}_i$, i.e. p^e or q^e must be contained in $\tilde{Q}_i$. Therefore p^e or q^e is an element of $\tilde{Q}_i \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$, and $\tilde{Q}_i \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$ is primary. Moreover, for $i \neq j$ we have

$$\sqrt{\tilde{Q}_i \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]} \not\subseteq \sqrt{\tilde{Q}_j \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]},$$

otherwise we had $\tilde{Q}_i \subseteq \sqrt{\tilde{Q}_j}$, because $\tilde{Q}_i \subseteq \sqrt{\tilde{Q}_j}$ and $\tilde{Q}_i \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}] \subseteq \sqrt{\tilde{Q}_j \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]}$ can be verified by means of the same computation (cf. Becker and Weispfenning (1993, p. 268)). Hence

$$J \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}] = \bigcap_{i=1}^{l'''} (\tilde{Q}_i \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}])$$

is a minimal primary decomposition. As $J \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$ is of dimension zero its primary components are uniqe up to permutation, this implies (iii).

From $J_\mathbb{L} \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}] = \bigcap_{i=1}^{l''} \tilde{Q}_i$ we can conclude (ii), as the reduced Gröbner bases of $J_\mathbb{L}$ and $J_\mathbb{L} \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$ coincide.

Now let $\mathbb{K}(\mathbf{g})/\mathbb{L}$ be separable. As above we recognize $J_{\mathbb{L}} \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$ as zero-dimensional and radical. In particular, its primary components are maximal ideals containing the zero-dimensional ideal $J \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$. Therefore they must be contained in $\{P_1, \ldots, P_l\}$, and we have proved (i).
Now assume $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ to be separable (not necessarily algebraic); let $J_{\mathrm{alg}} \trianglelefteq \mathbb{K}(\mathbf{g})_{\mathrm{alg}}[\mathbf{Z}]$ be the ideal corresponding to the algebraic closure $\mathbb{K}(\mathbf{g})_{\mathrm{alg}}$ of $\mathbb{K}(\mathbf{g})$ in $\mathbb{K}(\mathbf{x})$. Clearly, we have the inclusion $J \cdot \mathbb{K}(\mathbf{g})_{\mathrm{alg}}[\mathbf{Z}] \subseteq J_{\mathrm{alg}}$; as the dimensions of the latter ideals are equal (Lemma 2.1) J_{alg} is minimal among primes containing $J \cdot \mathbb{K}(\mathbf{g})_{\mathrm{alg}}[\mathbf{Z}]$ and therefore an associated prime hereof. From $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})_{\mathrm{alg}}$ being separable and $\mathbb{K}(\mathbf{g})_{\mathrm{alg}}$ algebraically closed in $\mathbb{K}(\mathbf{x})$ we can deduce that for a prime ideal $P \trianglelefteq \mathbb{K}(\mathbf{g})_{\mathrm{alg}}[\mathbf{Z}]$ also $P \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$ is prime (Lemma 4.1 (ii)). As $\dim(J \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]) = \dim(J_{\mathrm{alg}} \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}])$ we identify in particular $J_{\mathrm{alg}} \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$ as an associated prime of $J \cdot \mathbb{K}(\mathbf{x})[\mathbf{Z}]$.□

Note that for the special case $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ algebraic, $\mathbb{L}$ the separable closure of $\mathbb{K}(\mathbf{g})$ in $\mathbb{K}(\mathbf{x})$ the situation is extraordinarily simple:

Remark 4.3. Let $\mathbb{K}(\mathbf{g})$, $Q_1, \ldots, Q_l$ be as in Lemma 4.2, $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ algebraic, $\mathbb{K}(\mathbf{g})_{\mathrm{sep}}$ the separable closure of $\mathbb{K}(\mathbf{g})$ in $\mathbb{K}(\mathbf{x})$.

Then there is a $\lambda \in \{1, \ldots, l\}$: After removing the elements of $\mathbb{K}$ the coefficients of a reduced Gröbner basis of Q_λ form the canonical generating set of $\mathbb{K}(\mathbf{g})_{\mathrm{sep}}$ as computed by Algorithm 1.8.

Proof. The claim follows trivially when inspecting the proof of Lemma 4.2 for the case $\mathbb{L} = \mathbb{K}(\mathbf{g})_{\mathrm{sep}}$. □

While Lemma 4.2 in principle can be used for computing all intermediate fields of a separable algebraic extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$, for the problem of computing a primary decomposition see, e.g. Becker and Weispfenning (1993, Section 8), Eisenbud *et al.* (1992), or Gianni *et al.* (1988), for practical purposes probabilistic approaches like guessing a primitive element of the extension $\mathbb{K}(\mathbf{x})/\mathbb{K}(\mathbf{g})$ and factoring the minimal polynomial hereof, may be preferable (for the problem of computing intermediate fields of a finite algebraic extension cf. also Lazard and Valibouze (1993), for instance).

4.2. (counter-)example: purely inseparable extensions

The importance of separability for the characterization of intermediate fields as given in Lemma 4.2 can be illustrated by a simple example: for the purely inseparable extension $\mathbb{F}_2(x)/\mathbb{F}_2(x^4)$ the corresponding primary decomposition is given by

$$\langle Z^4 - x^4 \rangle = \langle Z - x \rangle^4,$$

i.e. the intermediate field $\mathbb{F}_2(x^2)$ can neither be described as an intersection of associated primes ($\langle Z - x \rangle$) nor as an intersecton of primary components ($\langle Z^4 - x^4 \rangle$). Another example is given by the extension $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$: as there are infinitely many intermediate fields Lemma 4.2 obviously cannot be used to characterize all of them.

5. Some Practical Considerations

For practical purposes the most critical part in the algorithms proposed is the computation of a Gröbner basis of the ideal J. As usually a term order of "block type" (cf. Algorithms 1.8, 1.17) has to be used here it is recommendable to use basis conversion techniques as discussed in Collart *et al.* (1993) or Faugère *et al.* (1993) for speeding up computations by computing a Gröbner basis w. r. t. an "easy" (e.g. a graded reverse lexicographical) order first. Moreover, it can prove useful to avoid unnecessary reductions during Buchberger's algorithm, as reducing polynomials can be rather expensive when dealing with coefficients in $\mathbb{K}(\mathbf{x})$, note that, e.g. for determining field membership the use of a reduced Gröbner basis is not mandatory. Indicating this problem to Allan Steel resulted in the implementation of the function `GroebnerBasisUnreduced` for computing unreduced Gröbner bases in the computer algebra system Magma. To illustrate its use we give an example from invariant theory, computations were done with Magma V2.20-2 on a Sun Ultra-1 with 143 MHz: Let ζ_{23} be a primitive 23rd root of unity,

$$\left\langle \begin{pmatrix} \zeta_{23} & 0 \\ 0 & -\zeta_{23} \end{pmatrix}, \begin{pmatrix} 0 & \zeta_{23} \\ -1 & 0 \end{pmatrix} \right\rangle \leq \mathrm{GL}(2, \mathbb{Q}(\zeta_{23}))$$

the subgroup of $\mathrm{GL}(2, \mathbb{Q}(\zeta_{23}))$ generated by $\left(\begin{smallmatrix} \zeta_{23} & 0 \\ 0 & -\zeta_{23} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & \zeta_{23} \\ -1 & 0 \end{smallmatrix}\right)$. It consists of 184 elements, and its field of invariants over $\mathbb{Q}(\zeta_{23})$ is generated by

$$\begin{aligned}
&\{{x_1}^{46} + {x_2}^{46}, {x_1}^{44}{x_2}^2 + {\zeta_{23}}^{21}{x_1}^2{x_2}^{44}, {x_1}^{42}{x_2}^4 + {\zeta_{23}}^{19}{x_1}^4{x_2}^{42}, {x_1}^{40}{x_2}^6 + {\zeta_{23}}^{17}{x_1}^6{x_2}^{40},\\
&\ {x_1}^{38}{x_2}^8 + {\zeta_{23}}^{15}{x_1}^8{x_2}^{38}, {x_1}^{36}{x_2}^{10} + {\zeta_{23}}^{13}{x_1}^{10}{x_2}^{36}, {x_1}^{34}{x_2}^{12} + {\zeta_{23}}^{11}{x_1}^{12}{x_2}^{34},\\
&\ {x_1}^{32}{x_2}^{14} + {\zeta_{23}}^{9}{x_1}^{14}{x_2}^{32}, {x_1}^{30}{x_2}^{16} + {\zeta_{23}}^{7}{x_1}^{16}{x_2}^{30}, {x_1}^{28}{x_2}^{18} + {\zeta_{23}}^{5}{x_1}^{18}{x_2}^{28},\\
&\ {x_1}^{26}{x_2}^{20} + {\zeta_{23}}^{3}{x_1}^{20}{x_2}^{26}, {x_1}^{24}{x_2}^{22} + \zeta_{23}{x_1}^{22}{x_2}^{24}, {x_1}^{92} + {x_2}^{92}\}.
\end{aligned}$$

Computing a reduced Gröbner basis over $\mathbb{Q}(\zeta_{23})(x_1, x_2)$ of the corresponding ideal w. r. t. the graded reverse lexicographic order with $Z_1 > Z_2$ using the standard `GroebnerBasis` function in Magma V2.20-2 takes about 12 min. Using `GroebnerBasisUnreduced` instead, thereby trying to avoid unnecessary reductions, after about 1 min results in a (in this particular case already reduced) Gröbner basis consisting of three polynomials; each of these polynomials contains three terms. Computation of a reduced Gröbner basis by means of tag variables $T_1, \ldots, T_{13}$, using a graded reverse lexicographic order on both the $T_1, \ldots, T_{13}$ and the x_1, x_2 block, after about 15 min results in a set of 146 polynomials (as expected when dealing with coefficients in $\mathbb{Q}(\zeta_{23})$ only the use of `GroebnerBasisUnreduced` does not speed up the computation here).

Note that the latter example also meets the expectation that in case of being given a generating set of a field $\mathbb{K}(\mathbf{g})$ with cardinality greater than the transcendence degree of $\mathbb{K}(\mathbf{g})/\mathbb{K}$ doing without tag variables is promising; to give another example of this behaviour we specify a subfield $\mathbb{Q}(g_1(\mathbf{x}), \ldots, g_5(\mathbf{x}))$ of $\mathbb{Q}(x_1, x_2)$ by giving five generators:

$$\begin{aligned}
g_1(\mathbf{x}) = n_1(\mathbf{x})/d_1(\mathbf{x}) &= ({x_1}^3 + x_1x_2 - 2)/({x_1}^2 - x_2 - 1),\\
g_2(\mathbf{x}) = n_2(\mathbf{x})/d_2(\mathbf{x}) &= ({x_1}^2 + {x_1}^3x_2 + 7)/(x_1 - {x_1}^2{x_2}^2),\\
g_3(\mathbf{x}) &= {x_1}^2 + 3x_1x_2,\\
g_4(\mathbf{x}) &= x_1{x_2}^2 + 5x_1x_2,\\
g_5(\mathbf{x}) &= {x_1}^3x_2 - x_2.
\end{aligned}$$

Here finding a reduced Gröbner basis of

$$\langle n_1(\mathbf{Z}) - g_1(\mathbf{x})d_1(\mathbf{Z}), n_2(\mathbf{Z}) - g_2(\mathbf{x})d_2(\mathbf{Z}), g_3(\mathbf{Z}) - g_3(\mathbf{x}), g_4(\mathbf{Z}) - g_4(\mathbf{x}), g_5(\mathbf{Z}) - g_5(\mathbf{x})\rangle :$$

$$((Z_1{}^2 - Z_2 - 1) \cdot (Z_1 - Z_1{}^2 Z_2{}^2))^\infty \trianglelefteq \mathbb{Q}(x_1, x_2)[Z_1, Z_2]$$

w. r. t. the graded reverse lexicographical term order with $Z_1 > Z_2$ takes less than 1 s and identifies $\mathbb{Q}(g_1(\mathbf{x}), \ldots, g_5(\mathbf{x}))$ as being equal to $\mathbb{Q}(x_1, x_2)$ while the computation of a reduced Gröbner basis using tag variables takes about 24 min.

We remark that no examples using tag parameters (cf. Section 1.2.1) have been given, as there is no implementation of this method available at the moment, and comparing a prototypic implementation of this technique with the rather elaborate algorithms in existing computer algebra systems did not seem to be sensible, either.

Acknowledgements

We are indebted to Markus Grassl and Allan Steel for their valuable support concerning the computer algebra system MAGMA. Moreover, we would like to thank the referees for various helpful comments.

References

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

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

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

Bosma, W., Cannon, J. (1996). *Handbook of Magma Functions, Volume I–III.*. Sydney.

Collart, S., Kalkbrener, M., Mall, D. (1993). The Gröbner Walk. Technical Report, Department of Mathematics, Federal Institute of Technology, Zurich, Switzerland.

Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. New York, Springer.

Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct methods for primary decomposition. *Invent. Math.*, **110**, 207–235.

Faugère, J., Gianni, P., Lazard, D., Mora, T. (1993, October). Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comput.* **16**, 329–344.

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

Jacobson, N., editor (1983). *Emmy Noether: Gesammelte Abhandlungen = Collected Papers*. Berlin, Heidelberg, Springer.

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.

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

Lazard, D., Valibouze, A. (1993). *Computing Subfields: Reverse of the Primitive Element Problem*, Vol. 109 of *Progress in Mathematics*, pp. 163–176. Boston, Birkhäuser.

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

Shafarevich, I. R. (1994). *Basic Algebraic Geometry-1*, 2nd edition. Berlin, Heidelberg, Springer.

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

Winter, D. (1974). *The Structure of Fields*. Graduate Texts in Mathematics. New York, Springer.

Zippel, R. (1991). Rational function decomposition. In S. M. Watt, ed., *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC'91*, Baltimore, pp. 1–6. ACM Press.

At the time of writing the following references were available electronically:

Aagedal *et al.* (1996):
http://dynamics.bu.edu/InterJournal/papers/[15]_113096195133_.html
Becker and Weispfenning (1993), errata:
ftp://alice.fmi.uni-passau.de/pub/GroebnerBook/errata.ps.gz
Collart *et al.* (1993):
http://www.math.ethz.ch/~darms/WWW/gr7/publications/groebnerwalk.ps
Kemper (1993):
ftp://ftp.iwr.uni-heidelberg.de/pub/kemper/Papers/Field_extensions/fields.ps.gz
Kemper (1994):
ftp://ftp.iwr.uni-heidelberg.de/pub/kemper/Papers/PhD_thesis/diss.ps.gz

Originally Received 3 December 1996
Accepted 2 July 1998