Deciding Linear Disjointness of Finitely Generated Fields

Jörn Müller-Quade and Martin Rötteler[*]

Institut für Algorithmen und Kognitive Systeme
Universität Karlsruhe, Germany

muellerq@ira.uka.de

Abstract

The behaviour of two field extensions with respect to each other can be described by the notions of *linear disjointness* and *freeness*. This paper gives methods for effectively deciding *linear disjointness* and *freeness* for fields lying under a finitely generated field $k(X) = \mathrm{Quot}(k[X_1, \ldots, X_s]/\mathrm{I}(X))$. Furthermore the methods developed can be used to decide for two given fields if there exists a field over which they are *linear disjoint*. This field (if it exists) is always the intersection of the two fields given. Thus we are able to compute the intersection of finitely generated fields which are linear disjoint.

All methods used rely on a correspondence from (pairs of) fields to ideals namely the ideal of syzygies of the generators of one field which have coefficients lying in the other field. We thereby generalize existing correspondences associating single fields or field extensions to ideals. Our contribution concludes with an outlook to the problem of computing the intersection of fields in more general situations.

1 Introduction

Most algorithms for function fields make use of constructive methods from ideal theory by associating a certain ideal to the field in question. The first correspondence of fields and ideals, which allowed to exploit Gröbner basis techniques for problems concerning function fields, was given by SWEEDLER in his work on the return of the killer tag variables [10]. The paper [10] adapts the ideas of SHANNON and SWEEDLER [9] from k-algebras to fields. These methods were improved and implemented by KEMPER [5]. An approach for subfields of rational function fields working without tag variables was first presented at [2], improved in [7], and then generalized to arbitrary function fields in [8].

All algorithms developed so far dealt with single function fields or single field extensions. In this paper we will associate ideals to pairs of fields. To make this correspondence effective we use both approaches mentioned above. Ideals associated to pairs of fields enable us to study the mutual behaviour of field extensions. The properties we will focus on are *linear disjointness* and *freeness*.

The fields $k(\mathbf{x})$, $k(\mathbf{y})$, and $k(\mathbf{z})$ considered in this paper are generated over a field k of constants and are contained in a field $k(X)$ which is a field of rational functions on a variety, i. e., the quotient field of a ring of polynomials modulo the prime ideal $\mathrm{I}(X)$. For all statements concerning constructibility the fields $k(\mathbf{x}), k(\mathbf{y}), k(\mathbf{z})$, and $k(X)$ are assumed to be finitely generated over a computable field k.

The following definition is consistent with [6] and differs from the more general view in [3].

Definition 1 *Let $k(\mathbf{x})$ and $k(\mathbf{y})$ be extensions of a field $k(\mathbf{z})$ both contained in a field $k(X)$.*

1. *The field $k(\mathbf{x})$ is said to be* linear disjoint *from $k(\mathbf{y})$ over $k(\mathbf{z})$ iff every finite subset of $k(\mathbf{x})$ linearly independent over $k(\mathbf{z})$ is still linearly independent over $k(\mathbf{y})$.*
2. *The field $k(\mathbf{x})$ is called* free *from $k(\mathbf{y})$ over $k(\mathbf{z})$ iff every finite subset which is algebraically independent over $k(\mathbf{z})$ remains algebraically independent over $k(\mathbf{y})$.*

Unless explicitly stated otherwise the fields in discussion obey the following relations:

$$\begin{tikzcd}
 & k(X) \arrow[d, dash] & \\
 & k(\mathbf{x},\mathbf{y}) \arrow[dr, dash] \arrow[ddl, dash] & \\
 & & k(\mathbf{y}) \arrow[ddl, dash] \\
k(\mathbf{x}) \arrow[dr, dash] & & \\
 & k(\mathbf{x}) \cap k(\mathbf{y}) \arrow[d, dash] & \\
 & k(\mathbf{z}) \arrow[d, dash] & \\
 & k &
\end{tikzcd}$$

Given two fields $k(\mathbf{x})$, $k(\mathbf{y})$ we define the ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ of all syzygies the generators of $k(\mathbf{x})$ have over the field $k(\mathbf{y})$.

For fields finitely generated over a computable field k the first part of this paper will give an effective construction for $J_{k(\mathbf{x})/k(\mathbf{y})}$. In the special case of $k(\mathbf{y}) \leq k(\mathbf{x})$ methods from [8] will be applied for a shortcut computation of $J_{k(\mathbf{x})/k(\mathbf{y})}$.

Furthermore we will see that for finitely generated fields the question whether two fields $k(\mathbf{x})$ and $k(\mathbf{y})$ are free over a field $k(\mathbf{z})$ can be decided by inspecting the transcendence degrees of the extensions $k(\mathbf{x})/k(\mathbf{z})$ and $k(\mathbf{x}, \mathbf{y})/k(\mathbf{y})$. These degrees can be computed using the corresponding syzygy

[*] supported by a fund of the Lehrstuhl Prof. Dr. Th. Beth

ideals and the degrees are equal iff $k(\mathbf{x})$ and $k(\mathbf{y})$ are free over $k(\mathbf{z})$.

If two fields $k(\mathbf{x})$ and $k(\mathbf{y})$ are linear disjoint over $k(\mathbf{z})$ one can think of the extensions $k(\mathbf{z})(\mathbf{x})/k(\mathbf{z})$ and $k(\mathbf{y})(\mathbf{x})/k(\mathbf{y})$ as being similar. The correspondence between fields and ideals will make this intuition more precise: Both extensions are performed by a set $\{\mathbf{x}\}$ of generators and the syzygy ideals of these generators over $k(\mathbf{y})$ and $k(\mathbf{z})$ respectively have equal reduced Gröbner bases iff $k(\mathbf{x})$ and $k(\mathbf{y})$ are linear disjoint over $k(\mathbf{z})$.

Furthermore we show that the existence of a field $k(\mathbf{z})$ over which the fields $k(\mathbf{x})$ and $k(\mathbf{y})$ are linear disjoint implies $k(\mathbf{z}) = k(\mathbf{x}) \cap k(\mathbf{y})$. In this case the intersection of the fields $k(\mathbf{x})$ and $k(\mathbf{y})$ can be computed using the ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$. The methods presented thus not only allow to decide for finitely generated fields $k(\mathbf{x})$ and $k(\mathbf{y})$ if there exists a field $k(\mathbf{z})$ over which they are linear disjoint, but also to compute this field $k(\mathbf{z})$.

Finally we give an outlook to another important question concerning extensions $k(\mathbf{x})/k(\mathbf{z})$ and $k(\mathbf{y})/k(\mathbf{z})$ namely computing $k(\mathbf{x}) \cap k(\mathbf{y})$ in cases without linear disjointness. We will focus on separable extensions of function fields in one variable since we can give an additional criterion then.

2 The Ideal of Syzygies of the Field Generators

Given fields $k(\mathbf{x})$ and $k(\mathbf{y})$ lying over a field of constants and both being contained in some field $k(X)$ we formally define the syzygy ideal mentioned in the introduction.

Definition 2 *Let $k(\mathbf{x})$ and $k(\mathbf{y})$ be fields lying over a field k of constants and let $\{\mathbf{x}\}$, $\{\mathbf{y}\}$ denote the sets of generators of $k(\mathbf{x})$ and $k(\mathbf{y})$ over k respectively. Furthermore let $\bigcup_{x\in\{\mathbf{x}\}}\{Z_x\}$ be a set of variables and $k(\mathbf{y})[\mathbf{Z}]$ be the ring of polynomials in these variables over the field $k(\mathbf{y})$. Then the ideal $J_{k(\mathbf{x})/k(\mathbf{y})} \subseteq k(\mathbf{y})[\mathbf{Z}]$ of all algebraic relations of the set $\{\mathbf{x}\}$ over $k(\mathbf{y})$ is defined as*

$$\langle\{x - Z_x | x \in \{\mathbf{x}\}\}\rangle \cap k(\mathbf{y})[\mathbf{Z}].$$

The ideal $\langle\{x - Z_x | x \in \{\mathbf{x}\}\}\rangle$ used in the definition can also be viewed as a syzygy ideal, namely $J_{k(\mathbf{x})/k(\mathbf{x})}$ representing the trivial extension $k(\mathbf{x})/k(\mathbf{x})$.

The next lemma is the basis for the properties of the syzygies ideal which are used in the following.

Lemma 3 *The ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ equals the kernel of the specialization homomorphism*

$$\Psi_{\mathbf{x}} : k(\mathbf{y})[Z_{x_1}, \ldots, Z_{x_r}] \to k(\mathbf{y})(\mathbf{x}),$$

$$Z_x \mapsto x.$$

Proof: We show that

$$f(\mathbf{y}, \mathbf{Z}) \in \langle\{x - Z_x | x \in \{\mathbf{x}\}\}\rangle \cap k(\mathbf{y})[\mathbf{Z}] \text{ iff } f(\mathbf{y}, \mathbf{x}) = 0.$$

"$\Rightarrow$" This is obvious.
"$\Leftarrow$" To prove this implication we make use of a formula transformation which will also play an important rôle in the proofs of Lemma 5 and Proposition 8. Using a multi index ν the polynomial f can be written as

$$f(\mathbf{y}, \mathbf{Z}) = \sum_\nu \alpha_\nu \mathbf{Z}^\nu = \sum_\nu \alpha_\nu \prod_{i=1}^r Z_{x_i}^{\nu_i}.$$

Substituting Z_{x_i} by $x_i = (Z_{x_i} + (x_i - Z_{x_i}))$ we arrive at

$$f(\mathbf{y}, \mathbf{x}) = \sum_\nu \alpha_\nu \prod_{i=1}^r (Z_{x_i} + (x_i - Z_{x_i}))^{\nu_i} = 0$$

from which we would like to conclude $f(\mathbf{y}, \mathbf{Z}) \in \langle\{x - Z_x | x \in \{\mathbf{x}\}\}\rangle \cap k(\mathbf{y})[\mathbf{Z}]$. Expanding the product we get only one term of the sum not divisible by $(x_i - Z_{x_i})$ for some i. With $q_{j_\nu} \in k(\mathbf{x}, \mathbf{Z})$ suitably chosen we get:

$$f(\mathbf{y}, \mathbf{x}) = \sum_\nu \alpha_\nu \left(\prod_{i=1}^r Z_{x_i}^{\nu_i} + \sum_{j_\nu=1}^r q_{j_\nu}(x_{j_\nu} - Z_{x_{j_\nu}}) \right) = 0.$$

This is equivalent to

$$f(\mathbf{y}, \mathbf{x}) = f(\mathbf{y}, \mathbf{Z}) + \sum_\nu \alpha_\nu \sum_{j_\nu=1}^r q_{j_\nu}(x_{j_\nu} - Z_{x_{j_\nu}}) = 0$$

which immediately yields a representation of $f(\mathbf{y}, \mathbf{Z})$ in $\langle\{x - Z_x | x \in \{\mathbf{x}\}\}\rangle$ and we can conclude $f(\mathbf{y}, \mathbf{Z}) \in \langle\{x - Z_x | x \in \{\mathbf{x}\}\}\rangle \cap k(\mathbf{y})[\mathbf{Z}]$. ■

Let us first consider cases where one of the fields is the field k of constants. Let $k(\mathbf{x})$ be given as a field of rational functions on a variety X, i. e., as the quotient field of a ring of polynomials $k[X_1, \ldots, X_s]$ modulo a prime ideal $\mathrm{I}(X)$. Then the ideal $J_{k(\mathbf{x})/k}$ equals $\{p(Z_{X_1}, \ldots, Z_{X_s}) | p \in \mathrm{I}(X)\}$. In particular if $k(\mathbf{x})$ is a rational function field the ideal $J_{k(\mathbf{x})/k}$ is $\langle 0 \rangle$.

If the field $k(\mathbf{x})$ is given as a subfield of a field $k(X)$ of rational functions on a variety X, the ideal $J_{k(\mathbf{x})/k}$ can be computed using tag variables. For this purpose we first introduce another ideal. Using this construction it is important to distinguish between the free polynomial ring $k[X_1, \ldots, X_s]$ sometimes also written as $k[\mathbf{X}]$ and the coordinate ring $k[X] = k[\mathbf{X}]/I(X)$.

Definition 4 *Let the field $k(\mathbf{x})$ be a subfield of $k(X) = \mathrm{Quot}(k[X_1, \ldots, X_s]/\mathrm{I}(X))$ finitely generated over a field k and let $\overline{X}_1, \ldots, \overline{X}_s$ denote the residue classes of the variables $X_1, \ldots, X_s$ modulo $\mathrm{I}(X)$. Furthermore let*

$$x_1 = \frac{n_1(\overline{X}_1, \ldots, \overline{X}_s)}{d_1(\overline{X}_1, \ldots, \overline{X}_s)}, \ldots, x_r = \frac{n_r(\overline{X}_1, \ldots, \overline{X}_s)}{d_r(\overline{X}_1, \ldots, \overline{X}_s)}$$

be one possible representation of the generators of $k(\mathbf{x})$ in terms of the $\overline{X}_1, \ldots, \overline{X}_s$ — the generators of $k(X)$. For new variables $Z_{x_1}, \ldots, Z_{x_r}$, the variables $X_1, \ldots, X_s$ (in short $\mathbf{X}$), and $d = d_1(\mathbf{X}) \cdot \ldots \cdot d_r(\mathbf{X})$ — the product of the denominators — we define the ideal $T_{k(\mathbf{x})}$ as

$$(\langle n_1(\mathbf{X}) - d_1(\mathbf{X})Z_{x_1}, \ldots, n_r(\mathbf{X}) - d_r(\mathbf{X})Z_{x_r}\rangle + \mathrm{I}(X)) : d^\infty.$$

The above ideal is well defined as the next lemma will give a characterization which is independent of the particular choices made in Definition 4.

Lemma 5 *The ideal $T_{k(\mathbf{x})}$ is the kernel of the specialization homomorphism*

$$k[X_1, \ldots, X_s][\mathbf{Z}] \to k(X)$$

$$Z_{x_i} \mapsto x_i,\ X_i \mapsto \overline{X}_i.$$

Proof: We show that $f(X, \mathbf{Z}) \in T_{k(\mathbf{x})}$ is equivalent to $f(X, \mathbf{x}) = 0$.
"⇒": Let f be an element of $T_{k(\mathbf{x})}$. Then there is a $\mu \in \mathbb{N}$ such that

$$d^{\mu} f \in \left(\langle n_1(\mathbf{X}) - d_1(\mathbf{X}) Z_{x_1}, \ldots, n_r(\mathbf{X}) - d_r(\mathbf{X}) Z_{x_r}\rangle + \mathrm{I}(X)\right).$$

This implies the existence of $q \in \mathrm{I}(X), u_0, \ldots, u_r \in k[X][\mathbf{Z}]$ with $d^{\mu} f = u_0 + \sum_{i=1}^{r} u_i \cdot (n_i(\mathbf{X}) - x_i d_i(\mathbf{X}))$ and hence $(d^{\mu} f)(\mathbf{X}, \mathbf{x}) = 0$. Because of $d(\mathbf{X}, \mathbf{x})$ not lying in $\mathrm{I}(X)$ we get $f(\mathbf{X}, \mathbf{x}) = 0$.
"⇐": Given $f(\mathbf{X}, \mathbf{Z})$ with $f(\overline{X}_1, \ldots, \overline{X}_s, \mathbf{x}) = 0$. The constant "0" is understood as an element of $k(X) := \mathrm{Quot}(k[X]/\mathrm{I}(X))$, i.e., it is represented as $\frac{u}{v}$ with $u \in \mathrm{I}(X)$ and $v \notin \mathrm{I}(X)$. For the computations to come we fix the representation of the x_i in the X_j to the representation used in Definition 4 thereby eventually changing the result of $f(\mathbf{X}, \mathbf{x})$ to $\frac{\tilde{u}}{\tilde{v}}$ with $\tilde{u} \in \mathrm{I}(X)$ and $\tilde{v} \notin \mathrm{I}(X)$. As $\mathrm{I}(X)$ is a prime ideal and $\tilde{v}$ is not in $\mathrm{I}(X)$ the above condition can be written as $f(\mathbf{X}, \mathbf{x}) \in \mathrm{I}(X)$. Using multi indices μ, ν we write f analogously to Lemma 3 as

$$f(\mathbf{X}, \mathbf{Z}) = \sum_{\mu,\nu} \alpha_{\mu,\nu} \mathbf{X}^{\mu} \mathbf{Z}^{\nu} = \sum_{\mu,\nu} \alpha_{\mu,\nu} \mathbf{X}^{\mu} \prod_{i=1}^{r} Z_{x_i}^{\nu_i}.$$

Substituting the Z_{x_i} with x_i written as $Z_{x_i} + (x_i - Z_{x_i})$ results in

$$f(\mathbf{X}, \mathbf{x}) = \sum_{\mu,\nu} \alpha_{\mu,\nu} \mathbf{X}^{\mu} \prod_{i=1}^{r} (Z_{x_i} + (x_i - Z_{x_i}))^{\nu_i} \in \mathrm{I}(X).$$

We expand the product and get only one term of the sum not divisible by $(x_i - Z_{x_i})$ for some i. Hence with suitably chosen $q_{j_\nu} \in k[\mathbf{Z}][\mathbf{x}]$ the above formula reads:

$$\sum_{\mu,\nu} \alpha_{\mu,\nu} \mathbf{X}^{\mu} \left(\prod_{i=1}^{r} Z_{x_i}^{\nu_i} + \sum_{j_\nu = 1}^{r} q_{j_\nu} (x_{j_\nu} - Z_{x_{j_\nu}}) \right) \in \mathrm{I}(X).$$

Using distributivity the last condition can be written as:

$$f(\mathbf{Z}, \mathbf{X}) + \sum_{\mu,\nu} \alpha_{\mu,\nu} \mathbf{X}^{\mu} \left(\sum_{j_\nu = 1}^{r} q_{j_\nu} (x_{j_\nu} - Z_{x_{j_\nu}}) \right) \in \mathrm{I}(X).$$

Multiplication with d^{η} for some $\eta \in \mathbb{N}$ clears the denominators resulting from the specialization of $\mathbf{Z}$ to $\mathbf{x}$ and with suitably chosen $\tilde{q}_{j_\nu}$ we have:

$$d^{\eta} f + \sum_{\mu,\nu} \alpha_{\mu,\nu} \mathbf{X}^{\mu} \left(\sum_{j_\nu = 1}^{r} \tilde{q}_{j_\nu} (n_{j_\nu} - d_{j_\nu} Z_{x_{j_\nu}}) \right) \in \mathrm{I}(X).$$

Therefore $d^{\eta} f \in T_{k(\mathbf{x})}$ and due to the saturation with d we get $f \in T_{k(\mathbf{x})}$ as desired. ■

This characterization of the tag variable ideal shows the relation of $T_{k(\mathbf{x})}$ to the ideals of Definition 2. The ideal $T_{k(\mathbf{x})}$ lies in the ring $k[\mathbf{X}][\mathbf{Z}]$ whereas the ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ is defined in $k(\mathbf{y})[\mathbf{Z}]$. For $T_{k(\mathbf{x})}$ we change the ring $k[\mathbf{X}]$ to $k[X] = k[\mathbf{X}]/\mathrm{I}(X)$ hence changing the ideal $T_{k(\mathbf{x})}$ to $T_{k(\mathbf{x})} + \mathrm{I}(X)$. Then looking at what these ideals generate in $k(X)[\mathbf{Z}]$ we get from Lemma 3 and Lemma 5 the equation

$$\left(T_{k(\mathbf{x})} + \mathrm{I}(X)\right) \cdot k(X)[\mathbf{Z}] = J_{k(\mathbf{x})/k(\mathbf{x})} \cdot k(X)[\mathbf{Z}].$$

The advantage of the ideal $T_{k(\mathbf{x})}$ is the possibility to compute a Gröbner basis with respect to a term order obeying $X_1, \ldots, X_s \gg Z_{x_1}, \ldots, Z_{x_r}$ since the $X_1, \ldots, X_s$ can be treated as variables. This enables us to compute the ideal of all syzygies the generators have over the field k of constants by elimination (Theorem 1 [5]).

Corollary 6 *With the notions of Definition 4 we get:*

$$J_{k(\mathbf{x})/k} = T_{k(\mathbf{x})} \cap k[Z_{x_1}, \ldots, Z_{x_r}]$$

This method can be extended to compute the ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ for fields $k(\mathbf{x})$ and $k(\mathbf{y})$ finitely generated over the field of constants. One first computes the ideal of algebraic relations of the set $\{\mathbf{x}\} \cup \{\mathbf{y}\}$ over k, i.e., the ideal $J_{k(\mathbf{x},\mathbf{y})/k}$ using tag variables and then specializes each tag variable Z_y with $y \in \{\mathbf{y}\}$ to the generator y it stands for.

Proposition 7 *Let $\Phi_{\mathbf{y}}$ denote the specialization homomorphism*

$$\Phi_{\mathbf{y}} : k[Z_{x_1}, \ldots, Z_{x_r}, Z_{y_1}, \ldots, Z_{y_m}] \rightarrow k[Z_{x_1}, \ldots, Z_{x_r}](\mathbf{y}),$$
$$Z_{y_i} \mapsto y_i$$

then

$$J_{k(\mathbf{x})/k(\mathbf{y})} = \left\langle \Phi_{\mathbf{y}} \left(J_{k(\mathbf{x},\mathbf{y})/k} \right) \right\rangle.$$

Proof: The inclusion "⊇" is obvious with Lemma 3 as all elements of $\left\langle \Phi_{\mathbf{y}} \left(J_{k(\mathbf{x},\mathbf{y})/k} \right) \right\rangle$ evaluate to zero when the Z_{x_i} are substituted by the x_i. To show the inclusion "⊆" we take a syzygy $p \in J_{k(\mathbf{x})/k(\mathbf{y})}$. Clearing the denominators of p gives a polynomial $\tilde{p} \in k[\mathbf{x}][\mathbf{Z}]$ replacing the x_i of $\tilde{p}$ by Z_{x_i} we get a syzygy $\tilde{p}(Z_{x_1}, \ldots, Z_{x_r}, Z_{y_1}, \ldots, Z_{y_m})$ which must be an element of $J_{k(\mathbf{x},\mathbf{y})/k}$. The polynomial $\Phi_{\mathbf{y}}(\tilde{p})$ differs from p only by a constant factor. Thus $p \in \left\langle \Phi_{\mathbf{y}} \left(J_{k(\mathbf{x},\mathbf{y})/k} \right) \right\rangle$. ■

For the case of $k(\mathbf{x})$ being an extension of $k(\mathbf{y})$ we can express the generators of $k(\mathbf{y})$ in terms of the $x_1, \ldots, x_r$. In this case an alternative characterization of the ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ already exists and one can take a computational shortcut [8]. The main advantage of this approach is the independence of the number of variables involved from the number of generators of $k(\mathbf{y})$.

Proposition 8 *Let $k(\mathbf{y}) \leq k(\mathbf{x})$ be fields finitely generated over k and let the generators $y_1, \ldots, y_m$ of $k(\mathbf{y})$ over k be expressed in $\mathbf{x} = x_1 \ldots, x_r$ as $y_1 = \frac{n_1(\mathbf{x})}{d_1(\mathbf{x})}, \ldots, y_m = \frac{n_m(\mathbf{x})}{d_m(\mathbf{x})}$. Let $\mathbf{Z}$ denote $Z_{x_1}, \ldots, Z_{x_r}$ then we define an ideal $I = \left\langle n_1(\mathbf{Z}) - \frac{n_1(\mathbf{x})}{d_1(\mathbf{x})} d_1(\mathbf{Z}), \ldots, n_m(\mathbf{Z}) - \frac{n_m(\mathbf{x})}{d_m(\mathbf{x})} d_m(\mathbf{Z}) \right\rangle$ and for $d = d_1(\mathbf{Z}) \cdot \ldots \cdot d_m(\mathbf{Z})$ we get:*

$$J_{k(\mathbf{x})/k(\mathbf{y})} = \left(J_{k(\mathbf{x})/k} + I \right) : d^{\infty}.$$

Proof: The ideal I used in the construction of Proposition 8 depends on the representation of the generators of $k(\mathbf{y})$ in the $x_1, \ldots, x_r$. One result of this proof will therefore be the independence of $\left(J_{k(\mathbf{x})/k} + I \right) : d^{\infty}$ from that particular choice. Following Lemma 3 we have to show that

$$f(\mathbf{y}, \mathbf{Z}) \in \left(J_{k(\mathbf{x})/k} + I \right) : d^{\infty} \text{ iff } f(\mathbf{y}, \mathbf{x}) = 0$$

"⇒" Let f be an element of $\left(J_{k(\mathbf{x})/k}+I\right):d^{\infty}$. Then there exists a $\eta\in\mathbb{N}$ such that $d^{\eta}f\in I+J_{k(\mathbf{x})/k}$ and this implies $d^{\eta}f(\mathbf{y},\mathbf{x})=0$. Since $d(\mathbf{x})\neq 0$ we get $f(\mathbf{y},\mathbf{x})=0$.

"⇐" Given $f\in k(\mathbf{y})[\mathbf{Z}]$ with $f(\mathbf{y},\mathbf{x})=0$ we have to take into account that this "0" is an element of $k(\mathbf{x})$. Thus if we represent the generators of $k(\mathbf{y})$ in $x_1,\ldots,x_r$ and then substitute all x_i by their corresponding variables Z_{x_i} we get $f(\mathbf{y}(\mathbf{Z}),\mathbf{Z})=\frac{u}{v}$ with $u\in J_{k(\mathbf{x})/k}$ and $v\notin J_{k(\mathbf{x})/k}$. Fixing the representation of the generators of $k(\mathbf{y})$ in $x_1,\ldots,x_r$ to the representation used in Proposition 8 the value of $f(\mathbf{y}(\mathbf{Z}),\mathbf{Z})$ may be changed to $\frac{\tilde{u}}{\tilde{v}}$ with $\tilde{u}\in J_{k(\mathbf{x})/k}$ and $\tilde{v}\notin J_{k(\mathbf{x})/k}$. Hence $f(\mathbf{y}(\mathbf{Z}),\mathbf{Z})=\frac{\tilde{u}}{\tilde{v}}$ is a rational function in $\mathbf{Z}$ vanishing at $Z_{x_i}=x_i$. Multiplying $f(\mathbf{y}(\mathbf{Z}),\mathbf{Z})$ with a suitable $c\in k[\mathbf{y}(\mathbf{Z})]$ we get $\tilde{f}=c\cdot f\in k[\mathbf{y}(\mathbf{Z})][\mathbf{Z}]$. Rewriting $\tilde{f}(\mathbf{y}(\mathbf{Z}),\mathbf{Z})$ we get the condition that

$$\tilde{f}(y_1(\mathbf{x})+(y_1(\mathbf{Z})-y_1(\mathbf{x})),\ldots,y_m(\mathbf{x})+(y_m(\mathbf{Z})-y_m(\mathbf{x})),\mathbf{Z})$$

is a rational function in $\mathbf{Z}$ vanishing at $Z_{x_i}=x_i$. This function can also be written with multi indices μ,ν as

$$\sum_{\mu,\nu}\alpha_{\mu,\nu}\mathbf{Z}^{\mu}\prod_{i=1}^{r}(y_i(\mathbf{x})+(y_i(\mathbf{Z})-y_i(\mathbf{x})))^{\nu_i}.$$

Analogously to the proof of Lemma 3 we expand the product and find only one term of the sum not divisible by $(y_i(\mathbf{Z})-y_i(\mathbf{x}))$ for some i. Thus for suitably chosen $q_{j_\nu}\in k[\mathbf{y},\mathbf{y}(\mathbf{Z}),\mathbf{Z}]$ we have that

$$\sum_{\mu,\nu}\alpha_{\mu,\nu}\mathbf{Z}^{\mu}\left(\prod_{i=1}^{r}y_i(\mathbf{x})^{\nu_i}+\sum_{j_\nu=1}^{r}q_{j_\nu}(y_{j_\nu}(\mathbf{Z})-y_{j_\nu}(\mathbf{x}))\right)$$

vanishes at $Z_{x_i}=x_i$. And therefore

$$\tilde{f}+\sum_{\mu,\nu}\alpha_{\mu,\nu}\mathbf{Z}^{\mu}\cdot\sum_{j_\nu=1}^{r}q_{j_\nu}(y_{j_\nu}(\mathbf{Z})-y_{j_\nu}(\mathbf{x}))$$

also vanishes at $Z_{x_i}=x_i$. For an $\eta\in\mathbb{N}$ chosen large enough multiplication with $d(\mathbf{Z})^{\eta}$ can clear the denominators of the last formula. Hence

$$d(\mathbf{Z})^{\eta}\cdot\tilde{f}+d(\mathbf{Z})^{\eta}\cdot\sum_{\mu,\nu}\alpha_{\mu,\nu}\mathbf{Z}^{\mu}\cdot\sum_{j_\nu=1}^{r}q_{j_\nu}(y_{j_\nu}(\mathbf{Z})-y_{j_\nu}(\mathbf{x}))$$

is a polynomial vanishing at $Z_{x_i}=x_i$ thus it is an element of $J_{k(\mathbf{x})/k}$. As the last formula represents a polynomial in $\mathbf{Z}$ there are suitable $\tilde{q}_{j_\nu}\in k[\mathbf{y},\mathbf{Z}]$ such that the above element of $J_{k(\mathbf{x})/k}$ can be written as

$$d(\mathbf{Z})^{\eta}\cdot\tilde{f}+\sum_{\mu,\nu}\alpha_{\mu,\nu}\mathbf{Z}^{\mu}\cdot\sum_{j_\nu=1}^{r}\tilde{q}_{j_\nu}(n_{j_\nu}(\mathbf{Z})-y_{j_\nu}(\mathbf{x})d_{j_\nu}(\mathbf{Z})).$$

Hence $d(\mathbf{Z})^{\eta}\cdot\tilde{f}$ is an element of the ideal $\tilde{I}+J_{k(\mathbf{x})/k}$ where $\tilde{I}\subset k[\mathbf{y}][\mathbf{Z}]$ is defined by

$$\tilde{I}:=\left\langle n_1(\mathbf{Z})-\frac{n_1(\mathbf{x})}{d_1(\mathbf{x})}d_1(\mathbf{Z}),\ldots,n_m(\mathbf{Z})-\frac{n_m(\mathbf{x})}{d_m(\mathbf{x})}d_m(\mathbf{Z})\right\rangle.$$

Clearly $\tilde{I}\cdot k(\mathbf{y})[\mathbf{Z}]=I$. Viewing $\tilde{f}\in k[\mathbf{y}][\mathbf{Z}]$ as an element of $k(\mathbf{y})[\mathbf{Z}]$ we may divide by the above chosen $c\in k[\mathbf{y}]$ and get

$$f=c^{-1}\tilde{f}\in\left(J_{k(\mathbf{x})/k}+I\right):d^{\infty}$$

■

Three examples will show how the syzygy ideal looks in different situations.

Example 9 *1. If $k(\mathbf{x})$ is a rational function field we know $J_{k(\mathbf{x})/k}$ to be $\langle 0\rangle$. Furthermore if the field $k(\mathbf{y})$ is a subfield of $k(\mathbf{x})$ generated by polynomials $y_1,\ldots,y_m$ the ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ can — according to Proposition 8 — be written down directly as $\langle y_1(\mathbf{x})-y_1(\mathbf{Z}),\ldots,y_m(\mathbf{x})-y_m(\mathbf{Z}))\rangle$.*
For $\mathbb{C}(a^2+b^2,ab)\leq\mathbb{C}(a,b)$ we get the corresponding ideal $\left\langle a^2+b^2-(Z_a^2+Z_b^2),ab-Z_aZ_b\right\rangle$.

2. For $\mathbb{C}(\frac{a^2+b^2}{ab})\leq\mathbb{C}(\frac{a}{b})$ we have $\frac{(a/b)^2+1}{a/b}=\frac{a^2+b^2}{ab}$, and following Proposition 8 we get $\left\langle Z_{\frac{a}{b}}^2-Z_{\frac{a}{b}}\frac{(a/b)^2+1}{a/b}+1\right\rangle$ which is the ideal generated by the minimal polynomial of $\frac{a}{b}$ over $\mathbb{C}(\frac{a^2+b^2}{ab})$.

3. Let $\mathbb{C}(a,b,c)$ denote $\mathrm{Quot}(\mathbb{C}[a,b,c]/\langle abc-1\rangle)$. Consider the subfields $\mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab)$ and $\mathbb{C}(\frac{a}{b})$. Then the ideal $J_{\mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab,\frac{a}{b})/\mathbb{C}}$ is

$$\left\langle Z_{\frac{b^2}{a^2+ab^3+cb^2}}(Z_{\frac{a}{b}}^2Z_{ab}+Z_{ab}^2-1)-Z_{ab}\right\rangle$$

and the ideal $J_{\mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab)/\mathbb{C}(\frac{a}{b})}$ thus equals

$$\left\langle Z_{\frac{b^2}{a^2+ab^3+cb^2}}(\frac{a^2}{b^2}Z_{ab}+Z_{ab}^2-1)-Z_{ab}\right\rangle.$$

For an ideal I the saturation $I:d^{\infty}$ is effective ([1] Algorithm IDEALDIV2) and so is the problem of representing a field element in some generators [10, 5, 8]. Thus the ideals of Definition 4 and Proposition 8 can be achieved through Gröbner basis computations.

Corollary 10 *Let the fields $k(\mathbf{x}),k(\mathbf{y})$ be finitely generated over a computable field k and contained in a field $k(X)=\mathrm{Quot}(k[X_1,\ldots,X_s]/\mathrm{I}(X))$. Then the ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ can be computed effectively.*

Summarizing what is said above we list the properties we will refer to later.

Corollary 11 *For fields $k(\mathbf{x}),k(\mathbf{y}),k(\mathbf{z})$ finitely generated over k the following conditions hold.*

1. *$k(\mathbf{y})[\mathbf{x}]\simeq k(\mathbf{y})[Z_{x_1},\ldots,Z_{x_r}]/J_{k(\mathbf{x})/k(\mathbf{y})}$.*
2. *$k(\mathbf{y})(\mathbf{x})\simeq\mathrm{Quot}\left(k(\mathbf{y})[Z_{x_1},\ldots,Z_{x_r}]/J_{k(\mathbf{x})/k(\mathbf{y})}\right)$.*
3. *$\dim(J_{k(\mathbf{x})/k(\mathbf{y})})$ equals the transcendence degree of $k(\mathbf{y})(\mathbf{x})$ over $k(\mathbf{y})$.*
4. *The monomials of $k(\mathbf{y})[Z_{x_1},\ldots,Z_{x_r}]$ not reducible modulo a fixed Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{y})}$ form a basis for $k(\mathbf{y})[Z_{x_1},\ldots,Z_{x_r}]/J_{k(\mathbf{x})/k(\mathbf{y})}$ as a vector space over $k(\mathbf{y})$.*
5. *For $k(\mathbf{z})\leq k(\mathbf{x})$ the coefficients of a reduced Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{z})}$ generate $k(\mathbf{z})$.*

Proof: With Lemma 3 we can directly conclude the points 1. and 2. of the corollary. To prove point 3. we follow the proof of Lemma 2 in [8]. The ideal $J_{k(\mathbf{x})/k(\mathbf{y})}$ is prime, and hence every maximally independent set S modulo $J_{k(\mathbf{x})/k(\mathbf{y})}$ has $\dim(J_{k(\mathbf{x})/k(\mathbf{y})})$ elements and the residue classes of the elements of S form in fact a maximal algebraic independent set over $k(\mathbf{y})$ ([1] Proposition 7.26 and Lemma 7.25). Point 4. is obvious from point 1. The property stated as point 5. is shown by Lemma 3 in [8] and the remark directly below it. ■

3 Deciding Freeness of Finitely Generated Fields

Lemma 12 *Let $k(\mathbf{x})/k(\mathbf{z})$ and $k(\mathbf{y})/k(\mathbf{z})$ be extensions of fields finitely generated over a field k of constants. Then $k(\mathbf{x})$ is free from $k(\mathbf{y})$ over $k(\mathbf{z})$ if and only if the transcendence degree of $k(\mathbf{x})/k(\mathbf{z})$ equals the transcendence degree of $k(\mathbf{y},\mathbf{x})/k(\mathbf{y})$.*

Proof: Assume the transcendence degree of $k(\mathbf{y},\mathbf{x})/k(\mathbf{y})$ to be smaller than the transcendence degree of $k(\mathbf{x})/k(\mathbf{z})$. Then a transcendence basis of the extension $k(\mathbf{x})/k(\mathbf{z})$ does not remain algebraically independent over $k(\mathbf{y})$ contradicting $k(\mathbf{x})$ being free from $k(\mathbf{y})$. The case that the transcendence degree of $k(\mathbf{y},\mathbf{x})/k(\mathbf{y})$ is larger than the transcendence degree of $k(\mathbf{x})/k(\mathbf{z})$ is impossible. ■

The next result will give a criterion based on the ideals associated to the field extensions of Lemma 12.

Proposition 13 *Let $k(\mathbf{x})/k(\mathbf{z})$ and $k(\mathbf{y})/k(\mathbf{z})$ be extensions of fields finitely generated over a field k of constants. Then the following conditions are equivalent:*

1. $\dim(J_{k(\mathbf{x})/k(\mathbf{z})}) = \dim(J_{k(\mathbf{x})/k(\mathbf{y})})$.
2. $\dim(J_{k(\mathbf{y})/k(\mathbf{z})}) = \dim(J_{k(\mathbf{y})/k(\mathbf{x})})$.
3. *The field $k(\mathbf{x})$ is free from $k(\mathbf{y})$ over $k(\mathbf{z})$.*

Proof: Obvious from Lemma 12 and point 3. of Corollary 11. ■

4 Deciding Linear Disjointness of Finitely Generated Fields

First we recall two criteria given in [6] Chapter X § 5.

Lemma 14
1. *$k(\mathbf{x})$ is linear disjoint from $k(\mathbf{y})$ over $k(\mathbf{z})$ iff every finite subset of $k[\mathbf{x}]$ which is linearly independent over $k(\mathbf{z})$ remains so over $k[\mathbf{y}]$.*
2. *$k(\mathbf{x})$ is linear disjoint from $k(\mathbf{y})$ over $k(\mathbf{z})$ iff there is a basis $\mathbf{b}$ of $k[\mathbf{x}]$ as a vector space over $k(\mathbf{z})$ which is linearly independent over $k[\mathbf{y}]$.*

Equipped with these and Corollary 11 we are able to state the main result of this section.

Proposition 15 *Let the fields $k(\mathbf{x})$ and $k(\mathbf{y})$ be finitely generated over a field k of constants. Then the following conditions are equivalent:*

1. *There exists a field $k(\mathbf{z})$ with $k(\mathbf{x})$ and $k(\mathbf{y})$ being linear disjoint over $k(\mathbf{z})$.*
2. *There exists a unique field $k(\mathbf{z})$ with $k(\mathbf{x})$ and $k(\mathbf{y})$ being linear disjoint over $k(\mathbf{z})$ and $k(\mathbf{z}) = k(\mathbf{x}) \cap k(\mathbf{y})$.*
3. $J_{k(\mathbf{x})/k(\mathbf{y})} = J_{k(\mathbf{x})/k(\mathbf{z})} \cdot k(\mathbf{y})[\mathbf{Z}]$.
4. $J_{k(\mathbf{y})/k(\mathbf{x})} = J_{k(\mathbf{y})/k(\mathbf{z})} \cdot k(\mathbf{x})[\mathbf{Z}]$.

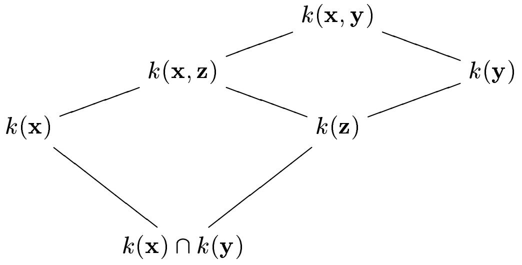
Proof: "1. ⇒ 2." Suppose $k(\mathbf{z}) < k(\mathbf{x}) \cap k(\mathbf{y})$ Then there exist elements from $k(\mathbf{x}) \cap k(\mathbf{y})$ linearly independent over $k(\mathbf{z})$ but not independent over $k(\mathbf{x}) \cap k(\mathbf{y})$. These elements are also elements of $k(\mathbf{x})$ which are linearly independent over $k(\mathbf{z})$ but not linearly independent over $k(\mathbf{y})$. Hence $k(\mathbf{x})$ cannot be linear disjoint from $k(\mathbf{y})$ over $k(\mathbf{z})$.
"2. ⇒ 1." This is obvious.
"3. ⇒ 1." The coefficients of a reduced Gröbner basis are elements of the smallest field possible since one could have started the Buchberger algorithm with a generating set having coefficients from this field and the algorithm does not need any field extensions. Thus the equation $J_{k(\mathbf{x})/k(\mathbf{y})} = J_{k(\mathbf{x})/k(\mathbf{z})} \cdot k(\mathbf{y})[\mathbf{Z}]$ implies that these ideals have equal reduced Gröbner bases. If we have equal reduced Gröbner basis for the ideals $J_{k(\mathbf{x})/k(\mathbf{y})}$ and $J_{k(\mathbf{x})/k(\mathbf{z})} \cdot k(\mathbf{y})[\mathbf{Z}]$ we also have equal vector space bases for the extensions $k(\mathbf{y})(\mathbf{x})/k(\mathbf{y})$ and $k(\mathbf{x})/k(\mathbf{z})$. Thus we can conclude the linear disjointness of $k(\mathbf{x})$ and $k(\mathbf{y})$ with point 2. from Lemma 14.
"1. ⇒ 3." Is proven via not 3. implies not 1. We have $J_{k(\mathbf{x})/k(\mathbf{z})} \cdot k(\mathbf{y})[\mathbf{Z}] \subset J_{k(\mathbf{x})/k(\mathbf{y})}$ and if these ideals are not equal they have different Gröbner bases. Since the ideals contain each other they also have different initial ideals. Thus we have monomials which can be reduced modulo a Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{y})}$ but cannot be reduced modulo a Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{z})} \cdot k(\mathbf{y})[\mathbf{Z}]$. According to point 4. of Corollary 11 we have a vector space basis of the extension $k(\mathbf{x})/k(\mathbf{z})$ which does not remain linearly independent over $k(\mathbf{y})$. This contradicts point 2. of Lemma 14 and therefore the fields $k(\mathbf{x})$ and $k(\mathbf{y})$ are not linear disjoint.
"4. ⇔ 1." This follows from the property of linear disjointness being symmetric (see [6] Chapter X § 5). ■

One interesting aspect of this result is the possibility to compute a generating set for the ideal $J_{k(\mathbf{y})/k(\mathbf{z})}$ without knowing $k(\mathbf{z})$ if the fields $k(\mathbf{x})$ and $k(\mathbf{y})$ are linear disjoint. Since we are able to extract the field $k(\mathbf{z})$ from the ideal $J_{k(\mathbf{y})/k(\mathbf{z})}$ we can compute the intersection of linear disjoint fields.

Corollary 16 *Let the fields $k(\mathbf{x})$ and $k(\mathbf{y})$ be finitely generated over a field k of constants and linear disjoint over their intersection. Then the set of coefficients of a reduced Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{y})}$ generates $k(\mathbf{x}) \cap k(\mathbf{y})$*

Proof: We have seen that the coefficients of a reduced Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{y})}$ $(= J_{k(\mathbf{x})/k(\mathbf{y}) \cap k(\mathbf{x})})$ must be contained in $k(\mathbf{x}) \cap k(\mathbf{y})$. The coefficients even generate this field according to point 5. of Corollary 11. ■

The methods developed above can also be applied to constructively answer the slightly more general question: *Given two fields $k(\mathbf{x}), k(\mathbf{y})$ does there exist a field $k(\mathbf{z}) \leq k(\mathbf{y})$ such that $k(\mathbf{z})(\mathbf{x})$ and $k(\mathbf{y})$ are linear disjoint over $k(\mathbf{z})$?*


$k(\mathbf{x},\mathbf{y})$
$k(\mathbf{x},\mathbf{z})$
$k(\mathbf{y})$
$k(\mathbf{x})$
$k(\mathbf{z})$
$k(\mathbf{x}) \cap k(\mathbf{y})$

Corollary 17 *For the fields $k(\mathbf{x}), k(\mathbf{y})$ finitely generated over k let $\{\mathbf{c}\}$ denote the set of coefficients of a reduced Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{y})}$. Then $k(\mathbf{x},\mathbf{c})$ is the minimal field lying over $k(\mathbf{x})$ such that $k(\mathbf{x},\mathbf{c})$ and $k(\mathbf{y})$ are linear disjoint.*

Example 18 *As in Example 9 let $\mathbb{C}(a,b,c)$ denote* $\mathrm{Quot}(\mathbb{C}[a,b,c]/\langle abc-1\rangle)$. *Again we consider the subfields $\mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab)$ and $\mathbb{C}(\frac{a}{b})$ and ask whether they are linear disjoint over some field $k(\mathbf{z})$. The ideal $J_{\mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab)/\mathbb{C}(\frac{a}{b})}$ was already computed to be*

$$\left\langle Z_{\frac{b^2}{a^2+ab^3+cb^2}}(Z_{ab}^2+\frac{a^2}{b^2}Z_{ab}-1)-Z_{ab}\right\rangle.$$

The generating set given already forms a reduced Gröbner basis. Thus there is only one coefficient ($\notin \mathbb{C}$) generating the field $\mathbb{C}(\frac{a^2}{b^2})$. With methods from [10, 5, 7] it is easy to check that $\mathbb{C}(\frac{a^2}{b^2}) \subset \mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab)$ and hence $\mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab) \cap \mathbb{C}(\frac{a}{b}) = \mathbb{C}(\frac{a^2}{b^2})$. Thus the fields $\mathbb{C}(\frac{b^2}{a^2+ab^3+cb^2},ab)$ and $\mathbb{C}(\frac{a}{b})$ are linear disjoint over $\mathbb{C}(\frac{a^2}{b^2})$.

5 An Outlook to the Intersection of Function Fields

In this section we show some cases where the methods developed so far allow the computation of the intersection of two fields even in the absence of linear disjointness. But we also want to point out that intersecting fields is a difficult task.

First we need some aid from Galois theory.

Lemma 19 *For fields $k(\mathbf{x}), k(\mathbf{y})$ lying over $k(\mathbf{z})$ let the extension $k(\mathbf{x})/k(\mathbf{z})$ be finite and Galois. Then $k(\mathbf{x})$ and $k(\mathbf{y})$ are linear disjoint over $k(\mathbf{x}) \cap k(\mathbf{y})$.*

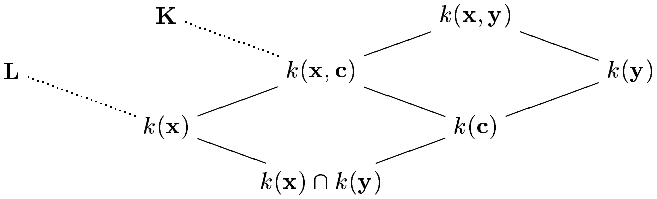
Proof: From [6] Chapter VIII Theorem 1.12. we know that the Galois group of the extension $k(\mathbf{x})/k(\mathbf{x}) \cap k(\mathbf{y})$ is a restriction of the Galois group of $k(\mathbf{x},\mathbf{y})/k(\mathbf{y})$. From this we can conclude that the extensions have equal degree and can be performed by adjoining identical roots. Looking at the syzygy ideals of this set of roots and applying Proposition 15 linear disjointness follows. ∎

In the context of Lemma 19 Lang uses the words “It is suggestive to think of the opposite sides of a parallelogram [in a diagram of fields] as being equal.” We think this perfectly describes the situation of linear disjointness. We will use Lemma 19 to decide in some cases if the intersection of two fields lies transcendentally under their compositum.

Proposition 20 *Let $k(\mathbf{x})$ and $k(\mathbf{y})$ be function fields in one variable over a field k of characteristic zero and let $k(\mathbf{c})$ be the field generated by the coefficients of a reduced Gröbner basis of $J_{k(\mathbf{x})/k(\mathbf{y})}$. Then at least one of the following conditions hold:*

1. *The normal closure $\mathbf{K}$ of $k(\mathbf{x},\mathbf{c})$ over $k(\mathbf{x})$ equals the normal closure of $k(\mathbf{x},\mathbf{c})$ over $k(\mathbf{c})$ and the field $k(\mathbf{x}) \cap k(\mathbf{y})$ is the fixed field of the group generated by* $\mathrm{Aut}(\mathbf{K}/k(\mathbf{x})) \cup \mathrm{Aut}(\mathbf{K}/k(\mathbf{c}))$.
2. *The fields $k(\mathbf{x})$ and $k(\mathbf{y})$ are linear disjoint.*
3. *The field $k(\mathbf{x}) \cap k(\mathbf{y})$ lies algebraically over k.*

Proof: We show that if neither 2. nor 3. hold point 1. must be true. Given a situation where $k(\mathbf{x})$ and $k(\mathbf{y})$ are not linear disjoint and the field $k(\mathbf{x}) \cap k(\mathbf{y})$ lies algebraically below $k(\mathbf{x})$ and $k(\mathbf{y})$. Let $\mathbf{K}$ denote the normal closure of $k(\mathbf{x},\mathbf{c})$ over $k(\mathbf{c})$ and $\mathbf{L}$ denotes the normal closure of $k(\mathbf{x})$ over $k(\mathbf{x}) \cap k(\mathbf{y})$.


$\mathbf{K}$
$k(\mathbf{x},\mathbf{y})$
$\mathbf{L}$
$k(\mathbf{x},\mathbf{c})$
$k(\mathbf{y})$
$k(\mathbf{x})$
$k(\mathbf{c})$
$k(\mathbf{x}) \cap k(\mathbf{y})$

The field $k(\mathbf{x},\mathbf{c})$ is linear disjoint from $k(\mathbf{y})$ and minimal (over $k(\mathbf{x})$) with this property as Corollary 17 says. Furthermore by Lemma 19 $\mathbf{L}$ is linear disjoint from $k(\mathbf{y})$ and $\mathbf{L} \cap k(\mathbf{x},\mathbf{c})$ is linear disjoint from $k(\mathbf{y})$ according to Proposition 5.1 in Chapter X of [6]. But we have $\mathbf{L} \cap k(\mathbf{x},\mathbf{c}) \geq k(\mathbf{x},\mathbf{c})$ since $k(\mathbf{x},\mathbf{c})$ was minimal. The normal closure of $k(\mathbf{x})$ over $k(\mathbf{x}) \cap k(\mathbf{y})$ thus lies over $k(\mathbf{x},\mathbf{c})$ and therefore equals the normal closure of $k(\mathbf{x},\mathbf{c})$ over $k(\mathbf{c})$. Hence $\mathbf{K} = \mathbf{L}$ and we are in the situation of point 1. ∎

The intersection of function fields in one variable of characteristic zero can therefore either be computed with methods from Galois theory (point 1. of Proposition 20) or the methods developed here can be applied to find the intersection (points 2. and 3.). Example 22 demonstrates all situations mentioned in Proposition 20. To apply Galois theory to the intersection problem the Galois groups must be known as subgroups of the automorphism group of the normal closure in question. It is not sufficient to know the isomorphism class of the Galois group. The following Proposition shows how a Galois group can be found in a suitable representation.

Proposition 21 *For finitely generated fields $k(\mathbf{x})$ and $k(\mathbf{y})$ let $k(\mathbf{x})/k(\mathbf{y})$ be a finite Galois extension with Galois group $G \leq \mathrm{Aut}(k(\mathbf{x}))$. Then the ideals*

$$\langle Z_{x_1} - \sigma(x_1,\dots,x_r),\dots,Z_{x_r} - \sigma(x_1,\dots,x_r)\rangle \text{ for } \sigma \in G$$

are exactly the associated primes of $J_{k(\mathbf{x})/k(\mathbf{y})} \cdot k(\mathbf{x})[\mathbf{Z}]$.

Proof: It is easy to see that one associated prime of $J_{k(\mathbf{x})/k(\mathbf{y})} \cdot k(\mathbf{x})[\mathbf{Z}]$ must be $\langle Z_{x_1} - x_1,\dots,Z_{x_r} - x_r\rangle$. From Proposition 13.10’ in [4] we know that all primes lying over $J_{k(\mathbf{x})/k(\mathbf{y})}$ are conjugated by the Galois group. In particular the associated primes of $J_{k(\mathbf{x})/k(\mathbf{y})} \cdot k(\mathbf{x})[\mathbf{Z}]$ are all on the same Galois orbit as $\langle Z_{x_1} - x_1,\dots,Z_{x_r} - x_r\rangle$. Thus they are exactly the ideals $\langle Z_{x_1} - \sigma(x_1,\dots,x_r),\dots,Z_{x_r} - \sigma(x_1,\dots,x_r)\rangle$ for $\sigma \in G$. ∎

Another difficulty in applying Galois theory is to recognize infinite groups from their generators as $\mathrm{Aut}(\mathbf{K}/k(\mathbf{x})) \cup \mathrm{Aut}(\mathbf{K}/k(\mathbf{y}))$ may no more be finite. Note that the automorphisms need not be linear.

Example 22 *To illustrate Proposition 20 we consider the following univariate fields.*

1. *What is the intersection of $\mathbb{C}(x^2)$ and $\mathbb{C}(x^2+x)$? The syzygy ideal $J_{\mathbb{C}(x^2,x^2+x)/\mathbb{C}}$ is* $\left\langle -Z_{x^2+x}^2 + 2Z_{x^2}Z_{x^2+x} - Z_{x^2}^2 + Z_{x^2}^3\right\rangle$ *and $J_{\mathbb{C}(x^2+x)/\mathbb{C}(x^2)}$ therefore equals*

$\left\langle -Z_{x^2+x}^2 + 2x^2 Z_{x^2+x} - (x^2)^2 + (x^2)^3 \right\rangle$. The coefficient of Z_{x^2+x} is x^2 which is not contained in $\mathbb{C}(x^2+x)$ hence the coefficients do not generate the intersection of $\mathbb{C}(x^2)$ and $\mathbb{C}(x^2+x)$. This implies that there exists no field over which $\mathbb{C}(x^2)$ and $\mathbb{C}(x^2+x)$ are linear disjoint. A short computation shows that both extensions $\mathbb{C}(x)/\mathbb{C}(x^2)$ and $\mathbb{C}(x)/\mathbb{C}(x^2+x)$ have the same normal closure namely $\mathbb{C}(x)$ as both extensions are Galois. Applying Proposition 21 we get $J_{\mathbb{C}(x)/\mathbb{C}(x^2+x)} = \left\langle x^2 + x - Z_x^2 - Z_x \right\rangle = \langle Z_x - x\rangle \cap \langle Z_x - (-x+1)\rangle$ and the Galois group of $\mathbb{C}(x)/\mathbb{C}(x^2+x)$ can be read off as $\{x \mapsto x, x \mapsto -x+1\}$. The Galois group of $\mathbb{C}(x)/\mathbb{C}(x^2)$ is $\{x \mapsto x, x \mapsto -x\}$ and jointly these Galois groups generate an infinite group of automorphisms as it contains $x \mapsto x+1$. The only rational functions invariant under $x \mapsto x+1$ are constants and hence $\mathbb{C}(x^2) \cap \mathbb{C}(x^2+x) = \mathbb{C}$.

2. *Compute the intersection of $\mathbb{C}(x^2)$ and $\mathbb{C}(x^3+x)$. The syzygy ideal $J_{\mathbb{C}(x^2,x^3+x)/\mathbb{C}}$ equals $\left\langle 2Z_{x^2}^2 + Z_{x^2} - Z_{x^3+x}^2 + Z_{x^2}^3 \right\rangle$. Substituting the variable Z_{x^2} by x^2 we get $J_{\mathbb{C}(x^3+x)/\mathbb{C}(x^2)} = \left\langle 2(x^2)^2 + x^2 - Z_{x^3+x}^2 + (x^2)^3 \right\rangle$. The coefficients generate $\mathbb{C}(x^6 + 2x^4 + x^2)$ which can easily be recognized as being a subfield of $\mathbb{C}(x^2)$ as well as $\mathbb{C}(x^3+x)$. The fields given are thus linear disjoint over the field just computed and with Corollary 16 we conclude $\mathbb{C}(x^2) \cap \mathbb{C}(x^3+x) = \mathbb{C}(x^6+2x^4+x^2)$.*

3. *Calculate the intersection of $\mathbb{C}(x^2)$ and $\mathbb{C}(x^3+x^2)$. Computations as above show that $\mathbb{C}(x^2)$ and $\mathbb{C}(x^3+x^2)$ are not linear disjoint. The coefficients of $J_{\mathbb{C}(x^3+x^2)/\mathbb{C}(x^2)}$ generate $\mathbb{C}(x^2)$. Furthermore the extension $\mathbb{C}(x)/\mathbb{C}(x^2)$ is Galois but the extension $\mathbb{C}(x)/\mathbb{C}(x^3+x^2)$ is not. Thus these extensions have different normal closures and following Proposition 20 we get $\mathbb{C}(x^2) \cap \mathbb{C}(x^3+x^2) = \mathbb{C}$.*

6 Computations

This section shows some computations done with Maple V.4 on a Sun UltraSparc with 166MHz. The two examples we give are chosen from invariant theory.

As a first example we consider the dihedral groups D_{2n} and their invariant fields. As abstract groups they are defined by

$$D_{2n} := \{\sigma, \tau : \sigma^n = \tau^2 = 1, \sigma^\tau = \sigma^{-1}\}$$

and they admit the faithful two-dimensional irreducible representations given by

$$\sigma \longmapsto \begin{pmatrix} \omega_n & 0 \\ 0 & {\omega_n}^{-1} \end{pmatrix}, \tau \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where ω_n denotes a primitve n–th root of unity.

Using Lemma 19 we know $\mathbb{C}(a,b)^{\langle\sigma\rangle}$ and $\mathbb{C}(a,b)^{\langle\tau\rangle}$ to be linear disjoint. Thus the field $\mathbb{C}(a,b)^{\langle\sigma,\tau\rangle}$ can (for each n) be computed by intersecting the fields

$$\mathbb{C}(a,b)^{\langle\sigma\rangle} = \mathbb{C}(a^n, b^n, ab)$$

and

$$\mathbb{C}(a,b)^{\langle\tau\rangle} = \mathbb{C}(a+b, ab).$$

For calculating these intersections we applied Proposition 7 and Corollary 16. We got the well known generators $a^n + b^n$ and ab for $\mathbb{C}(a,b)^{\langle\sigma,\tau\rangle}$.

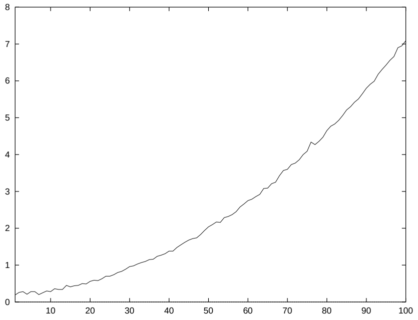


Figure 1: Timings for the dihedral groups D_{2n}.

Figure 1 shows the timings in seconds for $n = 1, \ldots, 100$. In this data we observe a subexponential growth of running time in the parameter n.

Another interesting family of groups is given by the (generalized) quaternion groups

$$Q_{4n} := \{\sigma, \tau : \sigma^n = \tau^2, \tau^4 = 1, \sigma^\tau = \sigma^{-1}\}$$

which admit the faithful two-dimensional irreducible representations given by

$$\sigma \longmapsto \begin{pmatrix} \omega_{2n} & 0 \\ 0 & {\omega_{2n}}^{-1} \end{pmatrix}, \tau \longmapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Applying the method above we can compute the field $\mathbb{C}(a,b)^{Q_{4n}}$ by intersecting the fields

$$\mathbb{C}(a,b)^{\langle\sigma\rangle} = \mathbb{C}(a^{2n}, b^{2n}, ab)$$

and

$$\mathbb{C}(a,b)^{\langle\tau\rangle} = \mathbb{C}(a^2b + ab^3, a^2 - b^2, a^4 + b^4).$$

The timings for our algorithm in this case are shown in Figure 2.

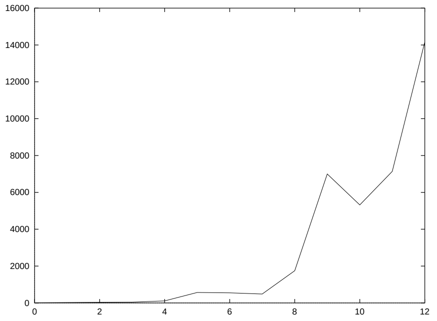


Figure 2: Timings for the quaternion groups Q_{4n}. For $n = 13$ the running time already was 53 310 s.

7 Conclusions

Given two fields $k(\mathbf{x})$ and $k(\mathbf{y})$ lying over a field $k(\mathbf{z})$ we can decide by means of Gröbner basis techniques whether

$k(\mathbf{x})$ is free resp. linear disjoint from $k(\mathbf{y})$ over $k(\mathbf{z})$. Furthermore the methods presented allow to compute a field $k(\mathbf{z})$ over which two given fields are linear disjoint if such a field exists. This field must be the intersection of the two fields given. Hence the intersection problem can be solved effectively in this situation even though the problem of intersecting finitely generated fields seems to be very difficult in general.

Acknowledgements

We thank Rainer Steinwandt for assistance from the distance and Prof. Dr. Th. Beth for helpful discussions. Furthermore we would like to thank our anonymous referee for his nice and helpful comments.

References

[1] Becker, T., and Weispfenning, V. *Gröbner Bases: A Computational Approach to Commutative Algebra.* In cooperation with Heinz Kredel. Graduate Texts in Mathematics. Springer, New York, 1993.

[2] Beth, T., Grassl, M., and Müller-Quade, J. Algebra for Optical Computing and Quantum Computing. In *The 2nd IMACS Conference on Applications of Computer Algebra* (RISC Hagenberg Österreich, July 1996). The proceedings contain abstracts only.

[3] Bürgisser, P., Clausen, M., and Shokrollahi, A. *Algebraic Complexity Theory.* No. 315 in Grundlehren der mathematischen Wissenschaften. Springer Verlag, 1997.

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

[5] Kemper, G. An Algorithm to Determine Properties of Field Extensions Lying over a Ground Field. IWR Preprint 93-58, Heidelberg, Oktober 1993. This paper is also contained in Gregor Kempers fields package for Maple.

[6] Lang, S. *Algebra*, 2 ed. Addison-Wesley, 1984.

[7] Müller-Quade, J., and Steinwandt, R. Basic Algorithms for Rational Function Fields. E.I.S.S.-Report 97-2 . E.I.S.S., Universität Karlsruhe, 1996.

[8] Müller-Quade, J., Steinwandt, R., and Beth, T. An application of Gröbner bases to the decomposition of rational mappings. In *Gröbner Bases and Applications (Proc. of the Conference 33 Years of Gröbner Bases)* (1998), B. Buchberger and F. Winkler, Eds., vol. 251 of *London Mathematical Society Lecture Notes Series*, Cambridge University Press.

[9] Shannon, D., and Sweedler, M. Using Gröbner Bases to Determine Algebra Membership, Split Surjective Homomorphisms Determine Birational Equivalence. *Journal of Symbolic Computation*, 6 (1988), 267–273.

[10] Sweedler, M. Using Groebner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: return of the killer tag variables. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 10th International Symposium, AAECC-10* (Berlin; Heidelberg, 1993), G. Cohen, T. Mora, and O. Moreno, Eds., vol. 673 of *LNCS*, Springer, pp. 66–75.