On the decomposition of rational functions

Mohamed Ayad and Peter Fleischmann

June 12, 2006

Abstract

Let $f := p/q \in \mathbb{K}(x)$ be a rational function in one variable. By Lüroth's theorem, the collection of intermediate fields $\mathbb{K}(f) \subsetneq \mathbb{L} \subsetneq \mathbb{K}(x)$ is in bijection with inequivalent proper decompositions $f = g \circ h$, with $g, h \in \mathbb{K}(x)$ of degrees ≥ 2. In (*Alonso, Gutierrez & Recio* 1995) an algorithm is presented to calculate such a function decomposition. In this paper we describe a simplification of this algorithm, avoiding expensive solutions of linear equations. A MAGMA implementation shows the efficiency of our method. We also prove some indecomposability criteria for rational functions, which were motivated by computational experiments.

1 Basic definitions and known results

Let $\mathbb{K}$ be an arbitrary field and $\mathbb{K}(x)$ the field of rational functions over $\mathbb{K}$. It is well known by Lüroth's theorem, that every intermediate field $\mathbb{L}$ with $\mathbb{K} \leq \mathbb{L} \leq \mathbb{K}(x)$ is of the form $\mathbb{K}(f)$ for some $f \in \mathbb{K}(x)$ (see (*Schinzel* 2000)). If $f := \frac{f_n}{f_d} \in \mathbb{K}(x)\backslash\mathbb{K}$ is a non-constant function with $f_n, f_d \in \mathbb{K}[x]$ coprime, then since f is transcendent over $\mathbb{K}$, the polynomial $m(y) := f_n(y) - f_d(y)f \in \mathbb{K}(f)[y]$ is irreducible with x as a zero. Hence

$$[\mathbb{K}(x) : \mathbb{K}(f)] = \max(\deg(f_n), \deg(f_d)) := \deg f,$$

which one calls the **degree of** f and denotes by $\deg(f)$.

Let $\mathbb{S} := \mathbb{K}(x)\backslash\mathbb{K}$ be the set of non-constant functions. Then $\mathbb{S}$ is equipped with a structure of a monoid, given by the **composition** $(f \circ g)(x) := f(g(x))$ for $f, g \in \mathbb{S}$. This monoid has a **right - action** on $\mathbb{K}(x)$ given by composition, i.e. for $f, g \in \mathbb{K}(x)$, $h, h' \in \mathbb{S}$ we have:

(a) $(f + g) \circ h = f \circ h + g \circ h$;

(b) $(f \cdot g) \circ h = (f \circ h) \cdot (g \circ h)$;

(c) $f \circ (h \circ h') = (f \circ h) \circ h'$ and

(d) x, the neutral element in $\mathbb{S}$, acts as identity operator.

Lemma 1.1. *For $g, h \in \mathbb{S}$ one has*

$$\deg(g \circ h) = \deg(g) \cdot \deg(h).$$

In particular $\circ$ is right - cancellable, i.e. for $f_1, f_2 \in \mathbb{S}$, $f_1 \circ h = f_2 \circ h$ implies $f_1 = f_2$.

Proof: The fields $\mathbb{K}(h)$ and $\mathbb{K}(x)$ are isomorphic, hence $[\mathbb{K}(h) : \mathbb{K}(g(h))] = [\mathbb{K}(x) : \mathbb{K}(g(x))]$ and we get

$$[\mathbb{K}(x) : \mathbb{K}(h)] \cdot [\mathbb{K}(x) : \mathbb{K}(g)] = [\mathbb{K}(x) : \mathbb{K}(h)] \cdot [\mathbb{K}(h) : \mathbb{K}(g(h))] = [\mathbb{K}(x) : \mathbb{K}(g \circ h)].$$

If $f_1 \circ h = f_2 \circ h$, then $(f_1 - f_2) \circ h = 0$ and a degree - argument shows that $f_1 - f_2$ is constant, hence zero. $\diamond$

From this it follows easily that the group of units with respect to composition is given by

$$\mathbb{U}_\circ := \{\frac{ax+b}{cx+d} \mid \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0\}.$$

Moreover the map

$$\varphi : \ \mathrm{GL}_2(\mathbb{K}) \to \mathbb{S}, \ \mathcal{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{ax+b}{cx+d}$$

is easily seen to be a homomorphism of monoids and therefore it induces an isomorphism

$$\mathrm{PGL}_2(\mathbb{K}) \cong \mathbb{U}_\circ.$$

It follows that there is a natural right action of $\mathrm{GL}_2(\mathbb{K})$ on $\mathbb{K}(x)$ via field - automorphisms over $\mathbb{K}$, given by $f^{\mathcal{M}} := f \circ \varphi(\mathcal{M})$. Let $A := \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(x))$ denote the full group of $\mathbb{K}$ - automorphisms of $\mathbb{K}(x)$ and $\alpha \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(x))$ with $x^\alpha = p(x)/q(x)$ in reduced form. Then $1 = \deg(x) = \deg(\alpha(x))$, hence $p(x) = ax + b$ and $q(x) = cx + d$ with $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$ and $f^\alpha(x) = f(\frac{ax+b}{cx+d})$ for an arbitrary $f \in \mathbb{K}(x)$. So the right action of $G := \mathrm{GL}_2(\mathbb{K})$ on $\mathbb{K}(x)$ induces canonical isomorphisms

$$\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(x)) \cong \mathrm{PGL}_2(\mathbb{K}) \cong \mathbb{U}_\circ.$$

There is also a natural left - action of $\mathrm{GL}_2(\mathbb{K})$ on $\mathbb{S}$ given by

$$\mathcal{M} \cdot f := \varphi(\mathcal{M}) \circ f.$$

It follows from right - cancellability of $\circ$, that this action is **fixed - point free**, i.e. $\mathcal{M} \cdot f = f$ for some $f \in \mathbb{S}$ implies that $\mathcal{M}$ is a scalar matrix in the centre of GL_2 and therefore acting trivially on $\mathbb{S}$.

Definition 1.2. *Let $f \in \mathbb{S}$. Then we define the following subsets of $\mathbb{S}$:*

$$R_f := \{h \in \mathbb{S} \mid \exists g \in \mathbb{S} \text{ with } f = g \circ h\};$$

$$L_f := \{g \in \mathbb{S} \mid \exists h \in \mathbb{S} \text{ with } f = g \circ h\}.$$

Note that for $f = g \circ h$ and $\alpha \in \mathbb{U}_\circ$ we have $f = g \circ \alpha \circ \alpha^{-1} \circ h$, so there is a right action of G or $\mathbb{U}_\circ$ on L_f and a left action on R_f. The following result shows the significance of these actions:

Theorem 1.3. . *Let $\mathbb{L}_i = \mathbb{K}(f_i)$ with $f_i \in \mathbb{S}$ for $i = 1, 2$ be two intermediate fields with $\mathbb{K} \leq \mathbb{L}_i \leq \mathbb{K}(x)$. Then*

(a) $\mathbb{L}_1 \leq \mathbb{L}_2$ if and only if $f_2 \in R_{f_1}$.

(b) $\mathbb{L}_2 = \mathbb{L}_1$ if and only if $f_2 = {}^{\alpha}f_1$ for some $\alpha \in G$.

(c) The $\mathbb{L}_i$ are conjugate over $\mathbb{K}$, ie. $\mathbb{L}_2 = \mathbb{L}_1^{\alpha}$ for $\alpha \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(x))$ if and only if $f_2 = u \circ f_1 \circ v$ for some $u, v \in \mathbb{U}_\circ$.

(d) For every $f \in \mathbb{S}$ the mapping $h \mapsto \mathbb{K}(h)$ induces a bijection between the set of intermediate fields $\mathbb{K}(f) \leq \mathbb{L} \leq \mathbb{K}(x)$ and the set R_f/G of left G - orbits on the set of right factors R_f.

Proof: If $\mathbb{K}(f_1) \leq \mathbb{K}(f_2)$ then clearly $f_1 = g \circ f_2$ for some $g \in \mathbb{S}$ which is uniquely determined by the f_i. If $\mathbb{L}_1 = \mathbb{L}_2$, then g is of degree one. On the other hand, if $f_1 = g \circ f_2$ with $g \in \mathbb{U}_\circ$, then clearly $\mathbb{L}_1 = \mathbb{L}_2$. Now the rest is clear. $\diamond$

In dealing with functional decompositions, we will often come across homogenization of functions.

Definition 1.4. *For $F \in \mathbb{K}[x]$ define the* **homogenization** *to be*

$$\mathcal{H}_F(x, y) := y^{\deg(F)} F(x/y) \in \mathbb{K}[x, y].$$

We will need the following lemma:

Lemma 1.5. *Let $R, S, P, Q \in \mathbb{K}[x]$ with $\gcd(R, S) = \gcd(P, Q) = 1$. Then the polynomials Q, $\mathcal{H}_R(P, Q)$ and $\mathcal{H}_S(P, Q)$ are pairwise coprime.*

Proof: see (*Schinzel* 2000),pg.18. $\diamond$

2 A normal form for subfield generators

Let $\mathbb{L} = \mathbb{K}(f)$ be an intermediate field. Since the generators $f \in \mathbb{S}$ are only determined up to (left) G - conjugacy, it may be useful to have a unique normal form for such a generator. This is provided by the next definition and proposition. As a matter of notation Gf will denote the left G - orbit of f in $\mathbb{S}$.

Definition 2.1. *A function $f = \frac{p}{q} \in \mathbb{S}$ is called in* **normal form** *or* **normalized**, *if $p, q \in \mathbb{K}[x]$ are monic and coprime, $p(0) = 0$ and either $\deg(p) > \deg(q)$ or $m := \deg(p) < \deg(q) =: n$ with $q = x^n + q_{n-1}x^{n-1} + \cdots + q_0$ and $q_m = 0$.*
The set of all functions in normal form will be denoted by $\mathcal{N}$ or $\mathcal{N}_{\mathbb{K}}$.

If $f = \frac{p}{q} \in \mathbb{S}$ is in normal form, then the polynomials p and q are uniquely determined.
For example $\frac{x^2}{x+1}$ is a generator in normal form of the field $\mathbb{K}(\frac{x^2}{x^2+x+1})$ and $\frac{x}{x^2+1}$ is a generator in normal form of the field $\mathbb{K}(\frac{x}{x^2+x+1})$. If $f := f_n x^n + \cdots + f_1 x + f_0 \in \mathbb{K}[x]$ is of degree n, then $\hat{f} := (1/f_n)(f - f_0)$ is a generator in normal form of $\mathbb{K}(f)$.

Proposition 2.2. *For every $f \in \mathbb{S}$ there is a unique $\hat{f} = p/q$ of normal form inside Gf. The polynomials p and q are uniquely determined by f and the properties in the definition 2.1.*

Proof: We first show the existence of $\hat{f}$ in $G \cdot f$. So let $f = p/q = \frac{p_m x^m + \cdots + p_0}{q_n x^n + \cdots + q_0}$ with $\deg(p) = m$, $\deg(q) = n$ and $\gcd(p, q) = 1$. Note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f = \frac{ap + bq}{cp + dq}$$

with $\mathcal{H}_{ax+b}(p, q) = ap + bq$ and $\mathcal{H}_{cx+d}(p, q) = cp + dq$ being coprime, by Lemma 1.5. Firstly we can assume that $p_0 = 0$: Assume otherwise; if $q_0 = 0$ we apply $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. If $p_0 q_0 \neq 0$ we can assume that $m \geq n$ and apply $\begin{pmatrix} -q_0/p_0 & 1 \\ 0 & 1 \end{pmatrix}$. Now if $m = n$, we apply $\begin{pmatrix} 1 & 0 \\ -q_m/p_m & 1 \end{pmatrix}$ to achieve $m > n$ and after applying $\begin{pmatrix} q_n/p_m & 0 \\ 0 & 1 \end{pmatrix}$ we can assume that p, q are monic, $p_0 = 0$, $(p, q) = 1$ and of different degree. If $m > n$ we have achieved the normal form; if $m < n$ the function $\begin{pmatrix} 1 & 0 \\ -q_m & 1 \end{pmatrix} \cdot f = \frac{p}{q - q_m p}$ will be in normal form.
Now we show the uniqueness. Let $f = p/q$ and $\hat{f} := \frac{ap+bq}{cp+dq} = p'/q'$ with

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$$

and suppose that f and $\hat{f}$ are both in normal form. We will show that this implies $b = c = 0 = a - d$, hence $f = \hat{f}$.
If $d = 0$, then $(ap+bq)q' = p'pc$, so $bq_0q'_0 = 0$ and $b = 0$, a contradiction. Hence $d \neq 0$ and $\hat{f}(0) = bq_0/dq_0 = 0$ implies $b = 0$. We get the equation $apq' = p'(cp + dq)$, which implies $p \mid p' \mid p$ and therefore $p = p'$, since these are monic polynomials; so $aq' = cp+dq$. Assume $\deg(p) = m > n = \deg(q)$. If $c \neq 0$, then $\deg(q') = \deg(p) = \deg(p')$, a contradiction. Hence $c = 0$ and $a = d$. If $\deg(p) = m < n = \deg(q)$, a comparison of coefficients at x^m shows $a \cdot 0 = c + 0$ and again we conclude $c = 0 = a - d$.
If $\hat{f} = p/q$ is the normal form of f, then it is clear from the above, that the monic polynomials p and q are uniquely determined by f. $\diamond$

Now Theorem 1.3 and Proposition 2.2 yield:

Corollary 2.3. *The function $f \mapsto \mathbb{K}(f)$ induces a bijection between the set of non-constant intermediate fields $\mathbb{K} < \mathbb{L} \leq \mathbb{K}(x)$ and the set $\mathcal{N}_{\mathbb{K}}$ of normalized rational functions.*
If $\mathbb{L} = \mathbb{K}(f)$ with $f \in \mathcal{N}_{\mathbb{K}}$, we call f the (unique) **normalized generator** *of $\mathbb{L}$.*

It is well known that the intermediate field $\mathbb{L}$ contains a non-constant polynomial if and only if it has a polynomial generator. This easily follows from the above, and it turns out, as might be expected, that the unique normalized generator is a polynomial:

Corollary 2.4. *Let $\mathbb{L} = \mathbb{K}(\hat{f})$ with $\hat{f}$ in normal form. Then $\mathbb{L}$ contains a non-constant polynomial, if and only if $\hat{f} \in \mathbb{K}[x]$.*

Proof: Let $h \in \mathbb{K}[x] \cap \mathbb{L}\backslash\mathbb{K}$ and $\hat{f} = p/q$ in normal form. Then $h = g \circ \hat{f}$ for some $g = u/v$ with coprime polynomials u and v. Then $h = \frac{\mathcal{H}_u(p,q)\cdot q^{-\deg(u)}}{\mathcal{H}_v(p,q)\cdot q^{-\deg(v)}}$ and $hq^{\deg(u)}\mathcal{H}_v(p,q) = q^{\deg(v)}\mathcal{H}_u(p,q)$. Now by Lemma 1.5 $\mathcal{H}_v(p,q)$ must be a constant. In general this does not imply that $v \in \mathbb{K}$, but in our situation this follows: let $v = v_s x^s + \cdots + v_0$ with $v_s \neq 0$, then $\mathcal{H}_v(p,q) = v_s p^s + v_{s-1}p^{s-1}q + \cdots + v_0 q^s$. Then $\mathcal{H}_v(p,q) = \mathcal{H}_v(p,q)(0) = v_0 q_0^s$. If $v_0 = 0$, then $v_s p^s \equiv 0 \bmod(q)$, in contradiction to $v_s \neq 0$. So $\mathcal{H}_v(p,q) = v_0 q_0^s \neq 0$. If $\deg(p) < \deg(q)$, then

$$0 = \deg(\mathcal{H}_v(p,q)) = \deg(v_0 q^s) = \deg(q) \Rightarrow s = 0$$

and if $\deg(p) > \deg(q)$, then

$$0 = \deg(\mathcal{H}_v(p,q)) = \deg(v_s p^s) = \deg(p) \ \Rightarrow s = 0.$$

Hence $v \in \mathbb{K}$. Now it follows that

$$hq^{\deg(u)}v_0 = \mathcal{H}_u(p,q).$$

Since $h \notin \mathbb{K}$, we have that $u \notin \mathbb{K}$, so $\deg(u) > 0$ and Lemma 1.5 yields $q \in \mathbb{K}$, so $q = 1$. $\diamond$

3 An indecomposability criterion

Let $f = p/q$ be in the normal form of Definition 2.1. Then $p = x^\ell \widetilde{p}$ with $\ell > 0$ and $\widetilde{p}, q \in \mathbb{K}[x]$ monic with non-vanishing constant term. In this section we investigate the possible decompositions of f. It turns out that f is indecomposable, whenever $\widetilde{p}$ and q are irreducible with $\gcd(\ell, \deg(q)) = 1 = \gcd(\deg(\widetilde{p}), \deg(q))$ (see Proposition 3.5). If $\widetilde{p}$ and $q \in \mathbb{K}[x]$ satisfy $\widetilde{p}(x) = \hat{p}(x^k)$ and $q = \hat{q}(x^k)$ for some $1 < k \mid \ell \in \mathbb{N}$ and $\max\{\deg(\hat{p}), \deg(\hat{q})\} > 1$, then clearly $f = \frac{x^\ell \widetilde{p}}{q} = \frac{x^{\ell/k}\hat{p}}{\hat{q}}(x^k)$ is decomposable. If $\widetilde{p}$ and q are both irreducible with $\deg(q) < \deg(p)$, this is the only possibility how f could be decomposable see Proposition (3.5).

Normal form algorithm

Function **Normalize**()

Input: Fct $f = p/q$; // normalized

Output: normalized Fct $\hat{f}$, Matrix M with $\hat{f} = M \circ f$.

1. **local** Matrix M, U, Fct $\hat{f}$, Pol p, q, Int m, n;
2. $\hat{f} := f; p := \mathrm{Num}(\hat{f}); q := \mathrm{Denom}(\hat{f}); m := \mathrm{Deg}(p); n := \mathrm{Deg}(q)$;
3. $p_0 := \mathrm{Coeff}(p, 0); q_0 := \mathrm{Coeff}(q, 0)$;
4. if $p_0 \neq 0$ then // *want* $p_0 = 0$;
5. if $q_0 = 0$ then
6. $M := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $\hat{f} := M \cdot \hat{f}$;
7. else // *now* $p_0 \cdot q_0 \neq 0$
8. $U := \begin{pmatrix} -q_0/p_0 & 1 \\ 0 & 1 \end{pmatrix}$; $\hat{f} := U \circ \hat{f}; M := U \cdot M$;
9. end if;
10. end if; // *from now* $p_0 = 0$, $q_0 \neq 0$.
11. if $m = n$ then
12. $U := \begin{pmatrix} 1 & 0 \\ -q_n/p_m & 1 \end{pmatrix}$; $\hat{f} := U \circ \hat{f}; M := U \cdot M$;
13. end if; // *now* p, q *of different degrees.*
14. $U := \begin{pmatrix} q_n/p_m & 0 \\ 0 & 1 \end{pmatrix}$; $\hat{f} := U \circ \hat{f}; M := U \cdot M$; // *make p,q monic;*
15. if $m < n$ then
16. $U := \begin{pmatrix} 1 & 0 \\ -q_m & 1 \end{pmatrix}$; $\hat{f} := U \circ \hat{f}; M := U \cdot M$; // *remove* q_m*;*
17. end if;
18. return $\hat{f}, M$;
19. end function;

Definition 3.1. *Two polynomials $p, q \in \mathbb{K}[x]$ will be called ℓ* **- related**, *if $p(x) = \hat{p}(x^k)$ and $q(x) = \hat{q}(x^k)$ for $\hat{p}, \hat{q} \in \mathbb{K}[x]$ and $1 < k \mid \ell$. For $a, b \in \mathbb{K}[x]$, the symbol $a \sim b$ will denote that a and b are associated, ie. $b = \lambda a$ for some $0 \neq \lambda \in \mathbb{K}$.*

Note that if any two of the integers $\deg(p)$, $\deg(q)$ or ℓ are coprime, then p and q are not ℓ - related.

Proposition 3.2. *Let $\widetilde{p} \in \mathbb{K}[x]$ be irreducible and not associated to x; let $f = \frac{p}{q} \in \mathbb{K}(x)$ with $p = x^\ell \cdot \widetilde{p}$, $\ell > 0$, $\deg(p) \neq \deg(q)$, $\gcd(p, q) = 1$; f is not necessarily in normal form.*
Assume that $f = g \circ h$ is a proper decomposition. Then up to equivalence, $h = r/s$ with $r = x^k$, $k \mid \ell$ and $s(0) \neq 0$. Moreover $g := u/v$ with $u := u_\mu x^\mu + \cdots + u_{i_0} x^{i_0}$, $\mu := \deg(u)$, $i_0 := \min\{i \mid u_i \neq 0\} > 0$, $v := v_\nu x^\nu + \cdots + v_0$, $\nu := \deg(v)$, $v_0 \neq 0$, and one of the following holds:

I *$s = \widetilde{p}$, $k\mu = \ell$, $u = u_\mu \cdot x^\mu$, $\nu = \mu + 1$ and $q \sim \mathcal{H}_v(x^k, \widetilde{p}) = v_{\mu+1} x^{k(\mu+1)} + \cdots + v_0 \widetilde{p}^{\mu+1}$,*

$$\deg(p) < \deg(q) = \begin{cases} (\mu+1)k = \ell + k & \text{if } k > \deg(\widetilde{p}) \\ (\mu+1)\deg(\widetilde{p}) & \text{if } k < \deg(\widetilde{p}). \end{cases} \tag{1}$$

II *$p \sim \mathcal{H}_u(x^k, s)$, $q \sim s^{\mu-\nu}\mathcal{H}_v(x^k, s)$, $\ell = k i_0$, $\nu \leq \mu$,*

$$\widetilde{p} = u_\mu x^{k(\mu - i_0)} + u_{\mu-1} x^{k(\mu-i_0-1)} s + \cdots + u_{i_0} s^{\mu-i_0}; \tag{2}$$

$$q = s^{\mu-\nu} \cdot (v_\nu x^{k\nu} + v_{\nu-1} x^{k(\nu-1)} s + \cdots + v_0 s^\nu). \tag{3}$$

Moreover we have in case **II***:*

$$\deg(s) < \deg(r) = k \iff \deg(q) < \deg(p) = k\mu \text{ with } \mu > \nu; \tag{4}$$

$$\deg(s) > \deg(r) = k \iff \deg(q) = \mu \cdot \deg(s) > \deg(p) \tag{5}$$

with $\deg(\widetilde{p}) = \deg(s)(\mu - i_0)$.

Proof: Assume that $f = g \circ h$ is a proper decomposition. We can assume that $g = u/v$ with u, v coprime and $h = r/s$ is in normal form so $r(0) = 0$, $s(0) \neq 0$. With notation of Definition 1.4 and Lemma 1.5 we have

$$p \cdot \mathcal{H}_v(r, s) s^\mu = q \cdot \mathcal{H}_u(r, s) s^\nu, \tag{6}$$

with $s, \mathcal{H}_v(r, s), \mathcal{H}_u(r, s)$ pairwise coprime. Hence

$$\mathcal{H}_u(r, s) \mid p \mid \mathcal{H}_u(r, s) s^\nu \text{ and } \mathcal{H}_v(r, s) \mid q \mid \mathcal{H}_v(r, s) s^\mu.$$

Since x does not divide s, x^ℓ must be the exact x - power dividing $\mathcal{H}_u(r,s)$, hence $0 < i_0$ and $r \mid \mathcal{H}_u(r,s) \mid p$.
Assume first that r is not associate to a power of x. Then $\widetilde{p} \notin \mathbb{K}$ and $r = x^k \cdot \widetilde{p}$ for some $0 \leq k \leq \ell$. It follows that

$$\mathcal{H}_u(r,s) = u_\mu \cdot r^\mu + \cdots + u_{i_0} \cdot r^{i_0} s^{\mu - i_0},$$

with $\widetilde{p}^{i_0} \mid p$, so $i_0 = 1$, hence $k = \ell$ and $r = p \sim \mathcal{H}_u(r,s)$. Now equation (6) reads $\mathcal{H}_v(r,s)s^\mu \sim qs^\nu$, hence $\nu \leq \mu$. If $\deg(r) > \deg(s)$, then $\mu \cdot \deg(r) = \deg(p) = \deg(r)$, so $\mu = 1 \geq \nu$, a contradiction. If $\deg(r) < \deg(s)$, then $\deg(r) = \deg(p) = \deg(r) + (\mu - 1)\deg(s)$ and again we get the contradiction $\mu = 1 \geq \nu$. [1] We conclude that $r = x^k$ with $k \leq \ell$.
Now we assume that $\mathcal{H}_u(r,s)$ is not associated to p. Then $\widetilde{p} \notin \mathbb{K}$ and

$$x^\ell \sim \mathcal{H}_u(r,s) = x^{ki_0} \cdot \varphi$$

with $\varphi = u_\mu x^{k(\mu - i_0)} + \cdots + u_{i_0} s^{\mu - i_0}$. But $x \not| \varphi$ so $\varphi \in \mathbb{K}$ and since $\deg(r) \neq \deg(s)$, we conclude that $\mu = i_0$ and $u = u_\mu x^\mu$ with $k\mu = \ell$. Now equation (6) reads $\widetilde{p}\mathcal{H}_v(r,s)s^\mu \sim qs^\nu$, hence $\widetilde{p} \mid s$ and $\nu > \mu$. But $s^{\nu-\mu} \mid \widetilde{p}$, hence $\widetilde{p} = s$, $\nu = \mu + 1$ and $\deg(\widetilde{p}) \neq k$. It follows that $q = \mathcal{H}_v(x^k, \widetilde{p})$ with $\deg(q) = (\mu+1)k = \ell + k > \deg(p)$ if $k > \deg(\widetilde{p})$ and $\deg(q) = (\mu+1)\deg(\widetilde{p})$ if $k < \deg(\widetilde{p})$. Note that

$$k < \deg(\widetilde{p}) \iff \ell < \deg(\widetilde{p})\mu \iff \ell + \deg(\widetilde{p}) < (\mu+1)\deg(\widetilde{p}),$$

hence $\deg(q) > \deg(p)$ in both cases.
Now we assume that $p \sim \mathcal{H}_u(r,s) = u_\mu \cdot x^{k\mu} + \cdots + u_{i_0} \cdot x^{ki_0} s^{\mu - i_0}$ with $\ell = i_0 k$ and

$$\widetilde{p} \sim u_\mu \cdot x^{k(\mu - i_0)} + \cdots + u_{i_0} \cdot s^{\mu - i_0}.$$

Then equation (6) implies that $\nu \leq \mu$ and

$$q \sim \mathcal{H}_v(r,s)s^{\mu-\nu} = s^{\mu-\nu}(v_\nu \cdot x^{k\nu} + \cdots + v_0 \cdot s^\nu)$$

with $v_0 \sim q(0) \neq 0$. If $k > \deg(s)$, then $\deg(q) = k\nu + \deg(s)(\mu - \nu) < k\mu = \deg(p)$ and $\mu > \nu$. If $k < \deg(s)$, then

$$\deg(q) = \mu \cdot \deg(s) > \mu \cdot \deg(s) + i_0(k - \deg(s)) = \deg(s)(\mu - i_0) + i_0 k = \deg(p),$$

and $\deg(\widetilde{p}) = \deg(s)(\mu - i_0)$. $\diamond$

Remark 3.3. It is straightforward to construct decomposable examples for each of the situations described in Proposition 3.2:

[1] Here and in the following note that since $\deg(r) \neq \deg(s)$, the summands in the $\mathcal{H}_u(r,s)$ have pairwise different degrees, so $\deg(\mathcal{H}_u(r,s)) = \mu \cdot \deg(r)$ if $\deg(r) > \deg(s)$ and $i_0\deg(r) + (\mu - i_0)\deg(s)$ if $\deg(s) > \deg(r)$.

I : This case can be realized for any given irreducible polynomial $\widetilde{p} \in \mathbb{K}[x]$. Indeed, $s = \widetilde{p}$ is already determined. Now let $k \in \mathbb{N}$ be any positive integer different from $\deg(\widetilde{p})$ and set $r := x^k$ to determine $h := r/s$, define $\ell := k \cdot \mu$ for some $\mu \in \mathbb{N}$ and set $u := u_\mu x^\mu$. For any $v := v_{\mu+1}x^{\mu+1} + \cdots + v_0 \in \mathbb{K}[x]$ with $v_{\mu+1}v_0 \neq 0$, $v_{\mu+1} = 1$ if $k > \deg(\widetilde{p})$ and $v_0 = 1$ otherwise, the polynomial

$$q := \mathcal{H}_v(x^k, \widetilde{p}) = v_{\mu+1}x^{k(\mu+1)} + \cdots + v_0\widetilde{p}^{\mu+1}$$

is coprime to $p := x^\ell\widetilde{p}$, monic and of degree strictly larger that $\deg(p)$. Hence the rational functions $f := \frac{x^\ell\widetilde{p}}{q}$, $h = \frac{x^k}{\widetilde{p}}$ are reduced and satisfy $f = g \circ h$ with $g = \frac{u_\mu x^u}{v}$, where u_μ is a suitable scalar.

II : The occurence of these cases depends on special properties of $\widetilde{p}$. A necessary condition is that there are positive integers k, z, a polynomial $s \in \mathbb{K}[x]$ of degree different from k and scalars $a_0, a_1, \cdots, a_z \in \mathbb{K}$ such that $a_0 \cdot a_z \neq 0$ and $\widetilde{p}$ can be written in the form

$$\widetilde{p} = \sum_{j=0}^{z} a_j \cdot s^j x^{k(z-j)}. \tag{7}$$

If this is possible, we set $h := \frac{x^k}{s}$. Now let $\ell := k \cdot i_0$ be any multiple of k, set $\mu := z + i_0$ and $p := x^\ell \cdot \widetilde{p}$. If $\deg(s) < k$, define $u := \sum_{j=0}^{z} a_j x^{\mu-j}$ and choose $\nu < \mu$, if $\deg(s) > k$ then define $u := \sum_{j=i_0}^{\mu} a_{\mu-j}x^{\mu-j}$ and choose $\nu \leq \mu$.
Now search for $v := \sum_{m=0}^{\nu} v_m x^m \in \mathbb{K}[x]$ with $v_\nu \neq 0 \neq v_0$ such that the polynomial

$$q := \mathcal{H}_v(x^k, s) = s^{\mu-\nu}(v_\nu x^{k\nu} + v_{\nu-1}x^{k(\nu-1)}s + \cdots + v_0 s^\nu)$$

is coprime to $\widetilde{p}$. Then $f = g \circ h$ with $g := u/v$.

Example 3.4. *Let* $\mathbb{K} = \mathbb{F}_2$, $\widetilde{p} := x^3 + x + 1$, $s_1 := x + 1$, $k_1 := 3$, $z := 1$, $a_1 := 1 =: a_0$, $u := x^{i_0}(x + 1)$, $p_1 = x^{3i_0}(x^3 + x + 1)$, $\nu := 4 \leq 1 + i_0 = \mu$. *Let* $v := x^4 + x^3 + x^2 + x + 1$ *and*

$$q_1 := (x+1)^{i_0+1-4}(x^{12} + x^9(x+1) + x^6(x^2+1) + x^3(x+1)^3 + x^4 + 1) =$$

$$(x+1)^{i_0-3}(x^{12} + x^{10} + x^9 + x^8 + x^5 + x^3 + 1).$$

Then $\gcd(q_1, p_1) = 1$ *and* $f_1 = p_1/q_1 = (u/v) \circ (x^3/(x+1))$.
Let $s_2 = x^3+1$, $k_2 := 1$, $\ell = i_0 > 3$, $p_2 := x^{i_0}(x^3+x+1)$. *Note that* $\nu = 4 < \mu_2 = 1+i_0$. *For* $q_2 := (x^3+1)^{i_0-3}(x^4+x^3(x^3+1)+x^2(x^6+1)+x(x^3+1)^3+(x^3+1)^4) =$

$$(x^3+1)^{i_0-3}(x^{12} + x^{10} + x^8 + x^7 + x^6 + x^3 + x^2 + x + 1)$$

we have $\gcd(q_2, p_2) = 1$ *and* $f_2 := p_2/q_2 = g \circ h_2$ *with* $h_2 = x/(x^3 + 1)$.

Proposition 3.5. *Let $\widetilde{p} \in \mathbb{K}[x]$ be irreducible. Moreover let $\ell > 0$ and $f := p/q = \frac{x^\ell \widetilde{p}}{q}$ be a rational function as in Proposition 3.2, or in normal form. Then f is indecomposable in each of the following cases:*

(a) $\deg(q) < \deg(p)$ *and* $\gcd(\ell, \deg(\widetilde{p})) = 1$.

(b) $\deg(q) < \deg(p)$, *q is irreducible and $\widetilde{p}$ and q are not ℓ - related.*

(c) $\deg(q) > \deg(p)$, $\gcd(\ell, \deg(q)) \leq \deg(\widetilde{p})$ *and* $\gcd(\deg(q), \deg(\widetilde{p})) = 1$.

(d) q is irreducible of prime degree and $\widetilde{p}$ and q are not ℓ - related.

(e) q is irreducible with $\gcd(\ell, \deg(q)) = \gcd(\deg(\widetilde{p}), \deg(q)) = 1$.

Proof: Assume f is decomposable. In case (a), Proposition 3.2 shows that we are in situation **II** with $\deg(s) < k \mid \gcd(\deg(\widetilde{p}), \ell) = 1$, which is a contradiction.
Assume (b) holds. Again we are in situation **II** with $\deg(s) < k$; then $\mu > \nu$ and s divides q. If $s \sim 1$, then $1 < k$ and the equations (2) and (3) show that $\widetilde{p}$ and q are ℓ - related. Hence $q \sim s \notin \mathbb{K}$, $\mu = \nu + 1$ and $k\nu = 0$, which gives the contradiction $\nu = 0$ and $\mu = 1$.
Assume (c) holds. Then we are in situation **I** or in situation **II** with $\deg(s) > k$. Assume **I**: if $k > \deg(\widetilde{p})$, then we get the contradiction $k \mid \gcd(\ell, \deg(q)) \leq \deg(\widetilde{p})$. Hence

$$k < \deg(s) = \deg(\widetilde{p}) = \gcd(\deg(q), \deg(\widetilde{p})) = 1,$$

again a contradiction. So we are in situation **II** with

$$k < \deg(s) \mid \gcd(\deg(q), \deg(\widetilde{p})) = 1.$$

Assume (d) holds. Since $\deg(f) = \max(\deg(p), \deg(q))$, decomposibility of f requires $\deg(q) < \deg(p)$ and (b) gives a contradiction.
Assume (e) holds. Then $\widetilde{p}$ and q are not ℓ - related and by (b) we have $\deg(q) > \deg(p) \geq 1$. This and (c) give the contradiction $0 < \deg(\widetilde{p}) < 1$. $\diamond$

Corollary 3.6. *Let $x \not\sim \widetilde{p} \in \mathbb{K}[x]$ be irreducible, $\ell > 0$ and $f := x^\ell \widetilde{p} \in \mathbb{K}[x]$ a polynomial. Then f is indecomposable, if and only if $\widetilde{p}(x)$ is not of the form $\hat{p}(x^k)$ with $\hat{p} \in \mathbb{K}[x]$ and $1 < k \mid \ell$.*

Proof: The given condition is equivalent to $\widetilde{p}$ and $q := 1$ not being ℓ - related. So the claim follows from Proposition 3.5. $\diamond$

4 A simplified decomposition algorithm

From Theorem 1.3 it is clear that in order to describe the set of intermediate fields containing a given subfield $\mathbb{L} := \mathbb{K}(f)$, one has to know the set R_f of right factors of f. Assume we are given $\mathbb{L} \leq \mathbb{T} := \mathbb{K}(h)$ with $h \in R_f$. In order to express elements

of $\mathbb{L}$ explicitly as functions of h, we also have need to know the left factor $g \in \mathbb{K}(x)$ with $f = g \circ h$. Recall that g is uniquely determined by f and h.

In (*Alonso* et al. 1995) the authors describe algorithms to explicitly calculate this functional decomposition. We will briefly revisit these here with the aim of some simplifications. First we need the following easy lemma, which is also used in constructive proofs of Lüroth's theorem:

Lemma 4.1. *Let $u(x), v(x), F(x) \in \mathbb{K}[x]$, $v(x) \neq 0$ with $u(x) \neq \lambda v(x)$ for any $\lambda \in \mathbb{K}$ and let t be a new variable, algebraically independent of x. Then F is not divisible by $u(x) - tv(x)$ in the polynomial ring $\mathbb{K}(t)[x]$.*

Proof: Assume otherwise, then

$$\varphi(t) \cdot F(x) = A(t, x) \cdot (u(x) - tv(x))$$

with polynomials $\varphi \in \mathbb{K}[t]$ and $A \in \mathbb{K}[t, x]$. Let $c(x) \mid \gcd(F, u(x) - tv(x))$ and assume that $c(x)$ has positive degree. Then $u(\eta) = tv(\eta)$ for some root $\eta \in \overline{\mathbb{K}}$ of c, hence t is algebraic over $\mathbb{K}$. This contradiction shows that $\gcd(F, u(x) - tv(x)) = 1$. Considering roots of φ and the fact that u and v are linearly independent over $\mathbb{K}$ (and hence over $\overline{\mathbb{K}}$), we can also see that $\gcd(\varphi, u(x) - tv(x)) = 1$. This contradiction proves the lemma. $\diamond$

We will use the following definition of (*Alonso* et al. 1995)

Definition 4.2. *A bivariate polynomial $a(y, x) \in \mathbb{K}[y, x]$ is called* **near - separate**, *if it is of the form*

$$a(y, x) = \nabla_{p,q}(y, x) = p(y)q(x) - p(x)q(y) \tag{8}$$

with coprime polynomials $p(x), q(x) \in \mathbb{K}[x]$.

The following remarkable theorem has been proved in (*Alonso* et al. 1995). For convenience we will include their proof, because it is constructive and relevant for later algorithmic considerations:

Theorem 4.3. *Let $f = p/q, h = r/s \in \mathbb{S}$ with $1 = \gcd(p, q) = \gcd(r, s)$, then the following are equivalent:*

1. *$f = g \circ h$ for some $g \in \mathbb{K}(x)$.*
2. *$\nabla_{r,s}(y, x)$ divides $\nabla_{p,q}(y, x)$ in $\mathbb{K}[y, x]$.*

Proof: 1. $\Rightarrow$ 2.: The polynomials $r(y) - hs(y)$ and $p(y) - fq(y)$ are the minimal polynomials of x over $\mathbb{K}(h)$ and $\mathbb{K}(f)$, respectively. Since $\mathbb{K}(f) \leq \mathbb{K}(h)$, $r(y) - hs(y)$ divides $p(y) - fq(y)$ in $\mathbb{K}(h)[y]$, which yields an equation

$$q(x)(r(y)s(x) - r(x)s(y))\Psi = (p(y)q(x) - p(x)q(y))s(x)$$

with $\Psi \in \mathbb{K}(h)[y]$. The coefficients of Ψ are of the form $s^{\ell-k} \cdot \frac{a_k r^k + a_{k-1} r^{k-1} s + \cdots + a_0 s^k}{b_\ell r^\ell + b_{\ell-1} r^{\ell-1} s + \cdots + b_0 s^\ell}$, so after clearing denominators we get an equation of the form

$$\varphi(x)(r(y)s(x) - r(x)s(y)) = (p(y)q(x) - p(x)q(y))\chi(x)$$

with suitable univariate polynomials $\varphi, \chi \in \mathbb{K}[x]$. It is easily seen, that near - separate polynomials do not have non-trivial univariate factors, hence we conclude that $(r(y)s(x) - r(x)s(y))$ divides $(p(y)q(x) - p(x)q(y))$ in $\mathbb{K}[x, y]$.
2. $\Rightarrow$ 1.: Now assume that $\nabla_{r,s}(y, x)$ divides $\nabla_{p,q}(y, x)$ in $\mathbb{K}[y, x]$; then $r(y) - hs(y)$ divides $p(y) - fq(y)$ in $\mathbb{K}(x)[y]$. Let t be a new independent variable, then division by $r(y) - ts(y)$ inside $\mathbb{K}(t)[y]$ gives unique remainders $B(t, y) \equiv p(y) \bmod (r(y) - ts(y))$ and $D(t, y) \equiv q(y) \bmod (r(y) - ts(y))$ with $B, D \in \mathbb{K}(t)[y]$, such that $\deg_y(B)$ and $\deg_y(D)$ are less than $\deg_y(r(y) - ts(y)) = \deg(h)$. By Lemma 4.1, B and D are non-zero and

$$0 \equiv B(h, y) - fD(h, y) \equiv p(y) - fq(y) \bmod r(y) - hs(y) \in \mathbb{K}(x)[y].$$

Since $\deg_y(B(h, y) - fD(h, y)) < \deg_y(r(y) - hs(y)) = \deg(h)$, we get

$$0 = B(h, y) - f(x)D(h, y) \in \mathbb{K}(x)[y].$$

It follows that $\deg_y B = \deg_y D = k$, say, and we get for the leading terms B_k, D_k of $B, D \in \mathbb{K}(x)[y]$: $f(x) = B_k(h)/D_k(h) = g \circ h$ with $g(x) = B_k(x)/D_k(x)$. $\diamond$

Remark 4.4. Note that the steps in 2. $\Rightarrow$ 1. of Theorem 4.3 allow a direct construction of the left factor g, if a right factor h has been found: one simply has to divide $p(y)$ and $q(y)$ by $r(y) - ts(y)$ in $\mathbb{K}(t)[y]$, take the remainders $B(t, y)$ and $D(t, y)$, which have to be of the same y - degree k, and set $g(t) = B_k(t)/D_k(t)$.

It remains to find the right factor h. In (*Alonso* et al. 1995) it is proposed to first factorize $\nabla_{p,q}$ in $\mathbb{K}[y, x]$ and then check proper factors of the form $(y - x) \cdot a(y, x)$ for being near - separate, by solving certain linear systems of equations. We will now show that these linear systems can be completely replaced by a short and simple calculation. This is based on the following elementary observation:

Lemma 4.5. *Let $a(y, x) = \nabla_{u,v}(y, x)$ for $u(x), v(x) \in \mathbb{K}[x]$. Then the following identities hold in $\mathbb{K}[w, x, y, z]$:*

$$a(x, y) = -a(y, x) \tag{9}$$

$$a(w, x)a(y, z) + a(w, y)a(z, x) + a(w, z)a(x, y) = 0. \tag{10}$$

Conversely, assume that $a(y, x) \in \mathbb{K}[y, x]$ satisfies the identities (9) and (10), then

$$a(y, x) = \nabla_{u,v}(y, x) \text{ with } u(x) := a(x, \alpha) \text{ and } v(x) := \frac{a(x, \beta)}{a(\alpha, \beta)} \in \mathbb{K}[x] \tag{11}$$

for every $\alpha, \beta \in \mathbb{K}$ with $a(\alpha, \beta) \neq 0$.

Proof: Equation 9 is obvious. Equation 10 is of the form

$$(AB-CD)(FG-HE)+(AE-FD)(HB-CG)+(AG-HD)(CE-FB)=$$

$A\cdot 0+D\cdot 0=0$. The rest is clear. $\diamond$

If $0\neq a(y,x)$ is a divisor of $\nabla_{p,q}$ with $f=p/q$, then in order to decide if $a(y,x)$ is near-separate, we simply have to check the identities of Lemma 4.5. If they are satisfied and $a(y,x)$ does not vanish on $\mathbb{K}^2$ (e.g. whenever $\mathbb{K}$ is infinite), then Lemma 4.5 also provides polynomials $r(x),s(x)\in\mathbb{K}[x]$ with $a(y,x)=\nabla_{r,s}$. However, if $\mathbb{K}$ is a finite field, it can happen that $0\neq a(y,x)$ is zero on $\mathbb{K}^2$. If the identities of Lemma 4.5 hold, we can find $a(\alpha,\beta)\neq 0$ with $\alpha,\beta\in\overline{\mathbb{K}}$ and solve $a(y,x)=\nabla_{r,s}$ with $r,s\in\overline{\mathbb{K}}[x]$. But it is slightly more subtle to check and construct solutions over the ground field $\mathbb{K}$ (see Lemma 4.6 and equation (15)). For this analysis the following observation is useful:

Let $\mathbb{K}[y,x]/\mathbb{K}^*$ denote the set of bivariate polynomials modulo constants. Then the function $\nabla:\ \mathbb{S}\to\mathbb{K}[y,x]/\mathbb{K}^*$, mapping the reduced expression $f=p/q$ to the class $[\nabla_{p,q}]$, is constant on left G - orbits: indeed for $M=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in \mathrm{GL}_2$ we have $M\circ f=\frac{ap+bq}{cp+dq}$ with

$$\nabla_{ap+bq,cp+dq}=\det(M)\cdot\nabla_{p,q}. \tag{12}$$

Lemma 4.6. *Let $0\neq a(y,x)\in\mathbb{K}[y,x]$ with no univariate factors. Then the following are equivalent:*

1. *$a(y,x)=\nabla_{u,v}$ for two polynomials $u(x),v(x)\in\mathbb{K}[x]$.*
2. *There are $\alpha,\beta\in\overline{\mathbb{K}}$ such that $a(0,\alpha)\neq 0$ and $a(y,x)=\nabla_{r,\mathfrak{s}_{\alpha,\beta}}$ with $r(x):=a(x,0)$ and $\mathfrak{s}_{\alpha,\beta}(x):=\frac{a(\alpha,x)}{a(\alpha,0)}+\beta\cdot r(x)\in\mathbb{K}[x]$.*

Assume that 1. or 2. hold and let $r,s\in\mathbb{K}[x]$ with

$$a(y,x)=\nabla_{r,s}. \tag{13}$$

Then the total set of solutions $s'\in\mathbb{K}[x]$ of equation (13) with fixed r consists of all polynomials of the form $s'(x)=s(x)+c\cdot r(x)$ with $c\in\mathbb{K}$.
For any two pairs of solutions $(u(x),v(x))$, $(w(x),t(x))$ of equation (13), the corresponding functions $h:=u/v$ and $h':=w/t$ are equivalent, i.e. $h'=M\circ h$ with $M\in\mathrm{GL}_2(\mathbb{K})$.

Proof: 2. $\Rightarrow$ 1. is obvious.
1. $\Rightarrow$ 2.: By the assumption on $a(y,x)$, the polynomials u,v must be coprime. Hence the vector $(u(0),v(0))^{tr}$ is nonzero. Since SL_2 acts transitively on nonzero vectors, we can find $M\in\mathrm{SL}_2(\mathbb{L})$ such that $M\cdot(u(0),v(0))^{tr}=(0,1)^{tr}$. Now equation (12) shows that $a(y,x)=\nabla_{r,s}$ with $r(0)=0$, $s(0)=1$ and $r/s=M\circ u/v$. It follows that $r(x)=a(x,0)\neq 0$ and we can choose α as above. Now $a(\alpha,x)=a(\alpha,0)s(x)-r(x)s(\alpha)$,

Algorithm to decide near-separability of a and to solve $a = \nabla_{r,s}$

Function **Nearsep**()

Input: BivPol $a(y,x)$; // multiple of $y-x$;
// no univariate factors;

Output: Fct h; Int bool; // right factor $h = r/s$, if bool = 1:
// if $\mathbb{K}$ is finite, h can be defined in
// a suitable finite extension field.
// bool = 0, if $a(y,x)$ is not near separate.

1. **local** Fct h; Pol $r, \mathfrak{s}$; Int bool; Scalar α, m;
2. $r := a(x,0)$;
3. find α with $r(\alpha) =: m \neq 0$;// if $\mathbb{K}$ is finite, we need to search in extension fields
4. $\mathfrak{s}(x) := \frac{1}{m}a(\alpha,x)$;
5. if $a(y,x) = \nabla_{r,\mathfrak{s}}$ then **return** $h := \frac{r}{s}$, 1; end if;
6. **return** $h := x$, 0; // a is not near - separate, return function 'x' and the boolean '0'.
7. end function;

hence $s(x) = \frac{a(\alpha,x)}{a(\alpha,0)} + \beta r(x)$ with $\beta := \frac{s(\alpha)}{a(\alpha,0)}$.
Assume now that 1. and 2. hold. The operator $\nabla_{u,v}$ is bilinear in both arguments and $\nabla_{r,r} = 0$. It follows that for fixed r, any solution s and $c \in \mathbb{K}$, the combination $s + cr$ is again a solution of equation (13). On the other hand, if $\nabla_{r,s_0} = 0$ with $s_0 \in \mathbb{K}[x]$, then $s_0(x) = c \cdot r(x)$ for $c = s_0(\gamma)/r(\gamma)$ with suitable $\gamma \in \overline{\mathbb{K}}$. Hence $c \in \overline{\mathbb{K}} \cap \mathbb{K}(x) = \mathbb{K}$. So the set of all solutions with fixed numerator r is as described above.
Let (u,v), (w,t) be arbitrary solutions with corresponding functions h and h'. As in the beginning of this proof we can find elements $M, M' \in \mathrm{SL}_2(\mathbb{K})$ with $M \circ h = \frac{r}{s}$, $M' \circ h' = \frac{r}{s'}$ and $r(x) = a(x,0), s, s' \in \mathbb{K}[x]$ with $s(0) = s'(0)$. From the above we know that $s' = s + c \cdot r$ for suitable $c \in \mathbb{K}$, hence r/s' and r/s are equivalent and so are h' and h. $\diamond$

Now we assume that $\mathbb{K} = \mathbb{F}_q$, a finite field of order $q = p^s$. Let $0 \neq a(y,x) \in \mathbb{K}[y,x]$ have no univariate factors and suppose it satisfies the identities of Lemma 4.5, but vanishes on $\mathbb{K}^2$. If $a(y,x)$ is a divisor of $\nabla_{p,q}$ with normalized $f = p(x)/q(x) \in \mathbb{K}(x)$, then this implies that $p(x)$ and hence f vanish on $\mathbb{K}$, e.g. $f = \frac{x^2+x}{x^4+x+1} \in \mathbb{F}_2(x)$. Assume $a(\alpha,0) \neq 0$ with $\alpha \in \overline{\mathbb{K}}$, then $r := a(x,0)$ and $s_\alpha := \frac{a(\alpha,x)}{a(\alpha,0)}$ are solutions of equation (13). Clearly $r \in \mathbb{K}[x]$, but $s_\alpha \in \overline{\mathbb{K}}[x]$. By Lemma 4.6, there is a solution

Algorithm to compute the unique left factor g with $f = g \circ h$

Function **Leftfactor**()

Input: Fct $f = p(x)/q(x), h = r(x)/s(x)$; // reduced, $h \in R_f$.

Output: Fct g; // $f = g \circ h$,

1. **local** Fct g; Pol $F, B, C \in \mathbb{K}(x)[y]$;
2. $F(x, y) := r(y) - x \cdot s(y)$; // in $\mathbb{K}(x)[y]$;
3. $B(x, y) := p(y) \bmod F$; $C(x, y) := q(y) \bmod F$;
4. $g(x) :=$ LeadingCoefficient$_y(B)$/LeadingCoefficient$_y(D)$;
5. **return** $g(x)$;
6. end function;

$s \in \mathbb{K}[x]$ if and only if we can find $\beta \in \overline{\mathbb{K}}$ such that

$$s_\alpha(x) + \beta \cdot r(x) \in \mathbb{F}_q[x]. \tag{14}$$

Let $s_\alpha(x) = \alpha_m x^m + \cdots + \alpha_1 x + 1$, with $\alpha_i \in \overline{\mathbb{F}_q}$ and $r(x) = a_m x^m + \cdots + a_1 x$ with $a_i \in \mathbb{F}_q$ and $m \geq$ the maximum of both degrees. Such an element β satisfying equation (14) exists if and only if $\alpha_i + \beta \cdot a_i \in \mathbb{F}_q$, for all $i = 1, \cdots m$. This is equivalent to

$$\beta^q - \beta = \frac{\alpha_i - \alpha_i^q}{a_i} =: \gamma \text{ for all } i \text{ with } a_i \neq 0 \text{ and } \alpha_i \in \mathbb{F}_q, \text{ for all } i \text{ with } a_i = 0. \tag{15}$$

These conditions are easily verifiable and, if they are met, we can take β to be a root of $x^q - x - \gamma$.

Example 4.7. *Let $\mathbb{K} := \mathbb{F}_2$ and $f := (x^4 + x^2)/(x^2 + x + 1)$. Then we get the factorization $f := (x^2 + x) \circ \frac{x^2}{x+1}$, however the function Nearsep() needs to extend the field to $\mathbb{F}_4$ along the way.*

5 Complete decompositions, intermediate fields and examples

In this section we describe a MAGMA - implementation of an algorithm which determines all fields $\mathbb{L}$ with $\mathbb{K}(f) \leq \mathbb{L} \leq \mathbb{K}(x)$.

A sequence $\mathbf{g} := (g_m, g_{m-1}, \cdots, g_1)$ of elements $g_i \in \mathbb{K}(x)$ with $f = g_m \circ g_{m-1} \circ \cdots \circ g_1$ and $\deg(g_i) \geq 2$ is called a **decomposition** of f. Two decompositions

Algorithm to compute a generator f of the subfield $\mathbb{K}(g,h) \leq \mathbb{K}(x)$.

Function **Compfield()**

Input: Fct $g := g_n/g_d, h := h_n/h_d$;

Output: Fct f; normalized with $\mathbb{K}(f) = \mathbb{K}(g,h)$,

1. if deg(g) = 0 then return(Normalize(h)); end if;
2. if deg(h) = 0 then return(Normalize(g)); end if;
3. $m := \text{Min}(\deg(g), \deg(h))$;
4. $\Psi_g := g_n(z) - g \cdot g_d(z)$; $\Psi_h := h_n(z) - h \cdot h_d(z)$;
5. $DD := \text{Gcd}(\Psi_g, \Psi_h) \in \mathbb{K}(x)[z]$; $d := \deg_z(DD)$;//note that $DD \in \mathbb{K}(g,h)[z]$.
6. while $d < m$ do
7. for $i := 0$ to d do
8. if $\deg(\text{coeff}_{z^i}(DD)) > 0$ then
9. $q := \text{coeff}_{z^i}(DD)$; $q := \text{Normalize}(q)$;
10. $q_n := \text{Numerator}(q)$; $q_d := \text{Denominator}(q)$;
11. $\Psi_q := q_n(z) - q \cdot q_d(z)$;
12. $DD := \text{Gcd}(DD, \Psi_q); d := \deg_z(DD); m := \deg(q)$;
13. break;
14. end if;
15. end for;
16. end while;
17. return (Normalize(DD(0)));
18. end function;

$\mathbf{g} := (g_m, g_{m-1}, \cdots, g_1)$ and $\mathbf{h} := (h_n, h_{n-1}, \cdots, h_1)$ of f are called **equivalent** if $m = n$ and there are units $\alpha_1, \cdots, \alpha_{m-1} \in \mathbb{U}_\circ$ such that

$$g_m = h_m \circ \alpha_{m-1}^{-1}, g_{m-1} = \alpha_{m-1} \circ h_{m-1} \circ \alpha_{m-2}^{-1}, \cdots, g_i = \alpha_i \circ h_i \circ \alpha_{i-1}^{-1}, \cdots, g_1 = \alpha_1 \circ h_1.$$

The decomposition $\mathbf{g}$ is called a **full decomposition** iff all factors g_i are indecomposable and it is called **normal** if all factors $g_{m-1}, \cdots, g_1$, with the possible exception of g_m, are in normal form. It follows from Definition 2.1 that for every decomposition $\mathbf{g}$ of f there is a unique normal one which is equivalent to $\mathbf{g}$.

For the decomposition $\mathbf{g}$ of f and $i = 1, \cdots, m$ define $\widetilde{g}_i := g_i \circ g_{i-1} \circ \cdots \circ g_1$ and the associate sequence of proper intermediate fields

$$\mathcal{S}_{\mathbf{g}} := (\mathbb{L}_{m-1}, \cdots, \mathbb{L}_i, \cdots, \mathbb{L}_1) \text{ with } \mathbb{K}(f) < \mathbb{L}_i := \mathbb{K}(\widetilde{g}_i) < \mathbb{K}(x).$$

It follows directly from Theorem 1.3 that for two decompositions $\mathbf{g}, \mathbf{h}$ of f we have $\mathcal{S}_{\mathbf{g}} = \mathcal{S}_{\mathbf{f}}$ if and only if $\mathbf{g}$ and $\mathbf{f}$ are equivalent and that $\mathcal{S}_{\mathbf{g}}$ is a maximal sequence of proper intermediate fields if and only if $\mathbf{g}$ is a full decomposition. In other words, the set of maximal sequences of proper intermediate fields between $\mathbb{K}(f)$ and $\mathbb{K}(x)$ is in bijection with the set of all normal, full decompositions of f.

For $h := u/v$ in reduced expression define ∇_h to be the class $[\nabla_{u,v}] \in \mathbb{K}[y, x]/\mathbb{K}^*$. We define divisibility of classes $[q], [r] \in \mathbb{K}[y, x]/\mathbb{K}^*$ in the obvious way, i.e. $[q] \mid [r]$ iff $q \mid r$ in $\mathbb{K}[y, x]$. Then, due to Theorem 4.3 we have

$$f = g_m \circ g_{m-1} \circ \cdots \circ g_1 \iff \nabla_{\widetilde{g}_1} \mid \nabla_{\widetilde{g}_2} \mid \cdots \mid \nabla_{\widetilde{g}_m} = \nabla_f,$$

and $\mathbf{g}$ is a full decomposition of f if and only if for every $i = 1, \cdots, m-1$ there are no proper near - separate divisors "between" $\nabla_{\widetilde{g}_i}$ and $\nabla_{\widetilde{g}_{i+1}}$. In other words, there is a bijection between the set of intermediate fields $\mathbb{L}_i = \mathbb{K}(\widetilde{g}_i)$ and the set of near separate divisors $\nabla_{\widetilde{g}_i}$ of ∇_f. Using the function **Nearsep**(), one can easily produce a complete list of these, once the full factorization of ∇_f is known.

Example 5.1. *Let* $\mathbb{K} = \mathbb{Q}$, $f := \frac{x^{16}+2x^{12}+x^8}{x^{24}-2x^{12}+1}$. *MAGMA produces the following list of irreducible factors with multiplicities of* ∇_f*:*

$$< x - y, 1 >,\ < x + y, 1 >,\ < x * y - 1, 1 >,\ < x * y + 1, 1 >,\ < x^2 + y^2, 1 >,$$
$$< x^2 * y^2 + 1, 1 >,\ < x^8 * y^4 + x^8 + x^4 * y^8 + x^4 + y^8 + y^4, 1 >,$$
$$< x^8 * y^8 + x^8 * y^4 + x^4 * y^8 + x^4 + y^4 + 1, 1 > .$$

Using **Nearsep**() *we obtain the exponent vectors (in terms of the above list) of all near - separate divisors of* ∇_f*, together with corresponding generators of intermediate fields:*

$$[1, 0, 0, 0, 0, 0, 0, 0], \qquad x,$$

$[1,1,0,0,0,0,0,0]$, x^2,
$[1,0,1,0,0,0,0,0]$, $x/(x^2+1)$,
$[1,0,0,1,0,0,0,0]$, $x/(x^2-1)$,
$[1,1,1,1,0,0,0,0]$, $x^2/(x^4+1)$,
$[1,1,0,0,1,0,0,0]$, x^4,
$[1,1,0,0,0,1,0,0]$, $x^2/(x^4-1)$,
$[1,1,1,1,1,1,0,0]$, $x^4/(x^8+1)$,
$[1,1,0,0,1,0,0,1]$, $(x^8+x^4)/(x^{12}-1)$,
$[1,1,1,1,1,1,1,1]$, $(x^{16}+2x^{12}+x^8)/(x^{24}-2x^{12}+1)$.

Recall that $\mathbb{K}(f) \leq \mathbb{K}(h) \iff \nabla_h \mid \nabla_f$, *hence the containment relations between subfields are reflected in the reverse "dominance - order" of exponent vectors, where* $v \prec w \iff v - w$ *is non-negative. So* $[1,1,1,1,1,1,0,0] \prec [1,1,0,0,1,0,0,0]$ *indicates that* $\mathbb{K}(\frac{x^4}{x^8+1}) \leq \mathbb{K}(x^4)$ *and* $[1,1,0,0,1,0,0,1] \not\prec [1,1,1,1,0,0,0,0]$ *shows that* $\mathbb{K}(\frac{x^8+x^4}{x^{12}-1})$ *is not contained in* $\mathbb{K}(\frac{x^2}{x^4+1})$.
The computation was performed in 0.470 CPU seconds on a Laptop - PC with CPU Pentium 4 2.80 GHz.
*In (*Alonso et al. *1995), Example 5.4, a non - normalized version of this example was considered. The calculation, performed with MAPLE, took 202.53 seconds for one full decomposition.*

Example 5.2. *The following example also appears in (*Alonso et al. *1995), Example 5.1.:* $f := f_n/f_d$ *with*

$$f_n := -(4x^6+9x^5-13x^4-12x^3+29x^2-17x-8)(x^3+x^2-2x+1)\cdot$$

$$(3x^3+5x^2-8x-3)(9x^6+29x^5-24x^4-90x^3+39x^2+37x+3);$$

$$f_d := 91x^{18}+803x^{17}+1634x^{16}-4230x^{15}-16526x^{14}+5744x^{13}+61317x^{12}+$$

$$6452x^{11}-117349x^{10}-23079x^9+111529x^8+27940x^7-34289x^6-$$

$$36809x^5+5132x^4+11548x^3+1021x^2-929x-167.$$

The normalizaion of f *is equal to* $N := N_n/N_d$ *with*

$$N_n := x^{18}+68203/8196x^{17}+87695/6147x^{16}-32675/683x^{15}-3378407/24588x^{14}+$$

$$532687/4098x^{13}+324203/683x^{12}-1916254/6147x^{11}-6713321/8196x^{10}+$$

$$5584523/8196x^9+1543365/2732x^8-4842583/6147x^7+1155847/8196x^6+$$

$$1528231/8196x^5-667808/6147x^4-100585/6147x^3+136280/6147x^2+12775/2732x;$$

$$N_d := x^{17}+49436/6735x^{16}+1212/449x^{15}-592253/6735x^{14}-59726/449x^{13}+$$

$$889368/2245x^{12}+5126696/6735x^{11}-2101079/2245x^{10}-4175731/2245x^9+$$

$$2950617/2245x^8+14668796/6735x^7-2312663/2245x^6-527851/449x^5+$$

$$2211184/6735x^4 + 1919492/6735x^3 - 146716/6735x^2 - 66477/2245x - 8196/2245.$$

There is a unique full normalized decomposition, which is calculated by our MAGMA implementation in 0.490 seconds:

$$[\frac{x^3 - 3805/4098x^2 + 9125/32784x}{x^2 + 515/898x - 17075/64656}, \frac{x^2 + 5/12x}{x + 4/15}, \frac{x^3 + 4/3x^2 - 7/3x}{x^2 - x - 3}].$$

*(In (*Alonso et al. *1995) a corresponding MAPLE calculation took 249.23 seconds.)*

Example 5.3. *Let $f := (x^4 - 8x)/(x^3 + 1)$. Over the rationals f has the unique full decomposition*

$$[(x^2 - 2x)/(x + 1), (x^2 + 4x)/(x + 1)].$$

Let $\mathbb{K} := \mathbb{Q}(\zeta)$ with ζ a primitive third root of unity. Then f has the three non - equivalent full decompositions:

$$[(x^2 - 2x)/(x + 1), (x^2 + 4x)/(x + 1)]$$

$$[(x^2 + (2\zeta + 2)x)/(x - \zeta - 1), (x^2 + (-4\zeta - 4)x)/(x - \zeta - 1)]$$

$$[(x^2 - 2\zeta x)/(x + \zeta), (x^2 + 4\zeta x)/(x + \zeta)].$$

Suppose $F, G, H \in \mathbb{K}[x]$ are polynomials with $H \in \mathbb{K}(F) \cap \mathbb{K}(G)$. If the characteristic of $\mathbb{K}$ does not divide the degree of H, then Engstrom's formula (see (*Schinzel* 2000), pg.18 and pg.23) tells us that

$$[\mathbb{K}(F) : \mathbb{K}(F) \cap \mathbb{K}(G)] = \frac{\mathrm{lcm}(\deg(F), \deg(G))}{\deg(F)} \text{ and}$$

$$[\mathbb{K}(F, G) : \mathbb{K}(F)] = \frac{\deg(F)}{\gcd(\deg(F), \deg(G))}.$$

The following is an immediate consequence:

Corollary 5.4. *Let $F \in \mathbb{K}[x]$ be a polynomial of degree coprime to the characteristic of $\mathbb{K}$. Then $F = g \circ h = g' \circ h'$ with $\deg(h) = \deg(h')$ implies that $\mathbb{K}(h) = \mathbb{K}(h')$. In particular, if h and h' are normalized, then $h = h'$.*

Proof: By Corollary 2.3 we can assume that F, h and h' are in normal form. Then by Corollary 2.4, h and h' are also polynomials. Since $F \in \mathbb{K}(h) \cap \mathbb{K}(h')$, Ritt's first theorem implies that

$$[\mathbb{K}(h, h') : \mathbb{K}(h)] = \frac{\deg(h)}{\gcd(\deg(h), \deg(h))} = 1,$$

hence $\mathbb{K}(h) = \mathbb{K}(h')$ and $h = h'$, again by 2.3. $\diamond$

The following example shows that the assumption on the characteristic of $\mathbb{K}$ cannot be ommitted, neither in Ritt's first theorem, nor in Corollary 5.4:

Example 5.5. *Let* $\mathbb{K} := \mathbb{F}_4 = \mathbb{F}_2(a)$ *with* $a^2 + a + 1 = 0$ *and* $f := x^4 + 1$. *Then* f *has precisely the three inequivalent full decompositions*

$$[[x^2 + x, x^2 + x], [x^2 + ax, x^2 + a^2x], [x^2 + a^2x, x^2 + ax]],$$

corresponding to three proper intermediate subfields of the same index in $\mathbb{K}(x)$.

If $F \in \mathbb{K}[x]$ is a polynomial of degree coprime to the characteristic of $\mathbb{K}$, then F is indecomposable if and only if it is indecomposable over any extension field of $\mathbb{K}$ (see (*Schinzel* 2000), Theorem 6, pg.20).
This is not necessarily true if $\deg(F) \cdot 1_{\mathbb{K}} = 0$, as can be seen by the example of the polynomial F, which has precisely the following three inequivalent decompositions over $\mathbb{F}_8 := \mathbb{F}_2(\eta)$ (with $\eta^3 + \eta + 1 = 0$):

$$F := x^4+x^2+x = (x^2+\eta^6x)\circ(x^2+\eta x) = (x^2+\eta^2x)\circ(x^2+\eta^5x) = (x^2+\eta^4x)\circ(x^2+\eta^3x),$$

(note that Example 3 in (*Schinzel* 2000) is stated incorrectly, since F is indecomposable over $\mathbb{F}_4$. However it appears correctly in (*Schinzel* 1982), pg. 15.

The polynomial

$$F := x^{16} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x$$

has only the following two decompositions over $\mathbb{F}_4 = \mathbb{F}_2(a)$:

$$[x^4 + ax^3 + a^2x^2 + x,\ x^4 + a^2x^3 + ax^2 + x], [x^4 + a^2x^3 + ax^2 + x,\ x^4 + ax^3 + a^2x^2 + x],$$

in particular F is indecomposable over $\mathbb{F}_2$. An exhaustive search using our implementaion shows that F is a binary polynomial of minimal degree indecomposable over $\mathbb{F}_2$ and decomposable over $\mathbb{F}_4$.

6 Conclusive Remark

All algorithms in this paper have been implemented and tested in the computer algebra system MAGMA, version V2.11-6 (*Cannon & Playoust* 2007). A synopsis and the full software can be obtained at

`http://www.kent.ac.uk/ims/personal/pf10/calais/decomp_synopsis.txt` and `http://www.kent.ac.uk/ims/personal/pf10/calais/decomp`, respectively.

References

[1] Cesar Alonso, Jaime Gutierrez, Tomas Recio, *A Rational Function Decomposition Algorithm by Near-separated Polynomials*, J. Symbolic Comput. **19** (1995), 527–544.

[2] John Cannon, Catherine Playoust, *Algebraic Programming with Magma I An Introduction to the Magma Language*, Springer, Berlin 2007.

[3] Andrzej Schinzel, *Selected Topics on Polynomials*, University of Michigan, Ann Arbor 1982.

[4] Andrzej Schinzel, *Polynomials with special regard to Reducibility*, Cambridge University Press, Cambridge 2000.