Building counterexamples to generalizations for rational functions of Ritt's decomposition Theorem

Jaime Gutierrez[a,1] David Sevilla[b,1]

[a]*Dpto. de Matemáticas, Estadística y Computación, Universidad de Cantabria, E–39071 Santander, Spain*

[b]*Dpt. of Computer Science and Software Engineering, University of Concordia, Montreal, Canada*

Abstract

The classical Ritt's Theorems state several properties of univariate polynomial decomposition. In this paper we present new counterexamples to the first Ritt theorem, which states the equality of length of decomposition chains of a polynomial, in the case of rational functions. Namely, we provide an explicit example of a rational function with coefficients in $\mathbb{Q}$ and two decompositions of different length.

Another aspect is the use of some techniques that could allow for other counterexamples, namely, relating groups and decompositions and using the fact that the alternating group A_4 has two subgroup chains of different lengths; and we provide more information about the generalizations of another property of polynomial decomposition: the stability of the base field. We also present an algorithm for computing the fixing group of a rational function providing the complexity over the rational number field.

1 Introduction

The starting point is the decomposition of polynomials and rational functions in one variable. First we will define the basic concepts of this topic.

Definition 1 *If $f = g \circ h$, $f, g, h \in \mathbb{K}(x)$, we call this a* decomposition of f in $\mathbb{K}(x)$ *and say that g is a* component on the left *of f and h is a* component on the right *of f. We call a decomposition* trivial *if any of the components is a unit with respect to decomposition.*

[1] Partially supported by Spain Ministry of Science grant MTM2004-07086

Given two decompositions $f = g_1 \circ h_1 = g_2 \circ h_2$ *of a rational function, we call them* equivalent *if there exists a unit* u *such that*

$$h_1 = u \circ h_2 \,, \qquad g_1 = g_2 \circ u^{-1},$$

where the inverse is taken with respect to composition.

Given a non–constant f*, we say that it is* indecomposable *if it is not a unit and all its decompositions are trivial.*

We define a complete *decomposition of* f *to be* $f = g_1 \circ \cdots \circ g_r$ *where* g_i *is indecomposable. The notion of equivalent complete decompositions is straightforward from the previous concepts.*

Given a non–constant rational function $f(x) \in \mathbb{K}(x)$ *where* $f(x) = f_N(x)/f_D(x)$ *with* $f_N, f_D \in \mathbb{K}[x]$ *and* $(f_N, f_D) = 1$*, we define the* degree *of* f *as*

$$\deg f = \max\{\deg f_N,\ \deg f_D\}.$$

We also define $\deg a = 0$ *for each* $a \in \mathbb{K}$*.*

Remark 2 *From now on, we will use the previous notation when we refer to the numerator and denominator of a rational function. Unless explicitly stated, we will take the numerator to be monic, even though multiplication by constants will not be relevant.*

The first of Ritt's Theorems states that all the decomposition chains of a polynomial that satisfies a certain condition have the same length. It is well known that the result is not true for rational functions, see for example []. Here we explore new techniques related to this, and include a counterexample in $\mathbb{Q}(x)$.

Another result in this fashion states that if a polynomial is indecomposable in a certain coefficient field, then it is also indecomposable in any extension of that field. This is also false for rational functions, see [4] and [1]. We look for bounds for the degree of the extension in which we need to take the coefficients if a rational function with coefficients in $\mathbb{Q}$ has a decomposition in a larger field. In this paper we present a computational approach to this question and our conclusions.

In Section 2 we study how to compute bounds for the minimal field that contains all the decompositions of a given rational function. In Section 3 we introduce several definitions and properties of groups related to rational functions, which we use in Section 4 to discuss the number of components in the rational case. In particular, we present an algorithm for computing fixing group of a rational function and we provide the complexity over the rational number field. Finally, in Section 4 we present an example of a degree 12 rational function with coefficients in $\mathbb{Q}$ and two decompositions of different length; as far as we know this is the first example in $\mathbb{Q}$ of this kind.

2 Extension of the coefficient field

Several algorithms for decomposing univariate rational functions are known, see for instance [18] and [1]. In all cases, the complexity of the algorithm grows enormously when the coefficient field is extended. A natural question about decomposition is whether it depends on the coefficient field, that is, the existence of polynomials or rational functions that are indecomposable in $\mathbb{K}(x)$ but have a decomposition in $\mathbb{F}(x)$ for some extension $\mathbb{F}$ of $\mathbb{K}$. Polynomials behave well under certain conditions, however in the rational case this is not true. We will try to shed some light on the rational case.

Definition 3 *$f \in \mathbb{K}[x]$ is* tame *when* char $\mathbb{K}$ *does not divide* deg f.

The next theorem shows that tame polynomials behave well under extension of the coefficient field, see [8]. It is based on the concept of *approximate root* of a polynomial, which always exists for tame polynomials, and is also the key to some other structural results in the tame polynomial case.

Theorem 4 *Let $f \in \mathbb{K}[x]$ be tame and $\mathbb{F} \supseteq \mathbb{K}$. Then f is indecomposable in $\mathbb{K}[x]$ if and only if it is indecomposable in $\mathbb{F}[x]$.*

The next example, presented in [1], shows that the previous result is false for rational functions.

Example 5 *Let*

$$f = \frac{\omega^3 x^4 - \omega^3 x^3 - 8x - 1}{2\omega^3 x^4 + \omega^3 x^3 - 16x + 1}$$

where $\omega \notin \mathbb{Q}$ but $\omega^3 \in \mathbb{Q} \setminus \{1\}$. It is easy to check that f is indecomposable in $\mathbb{Q}(x)$. However, $f = f_1 \circ f_2$ where

$$f_1 = \frac{x^2 + (4-\omega)x - \omega}{2x^2 + (8+\omega)x + \omega}, \qquad f_2 = \frac{x\omega(x\omega - 2)}{x\omega + 1}.$$

We can pose the following general problem:

Problem 6 *Given a function $f \in \mathbb{K}(x)$, compute a minimal field $\mathbb{F}$ such that* *every decomposition of f over an extension of $\mathbb{K}$ is equivalent to a decomposition over $\mathbb{F}$.*

It is clear that, by composing with units in $\mathbb{F}(x) \supseteq \mathbb{K}(x)$, we can always turn a given decomposition in $\mathbb{K}(x)$ into one in $\mathbb{F}(x)$. Our goal is to minimize this, that is, to determine fields that contain the smallest equivalent decompositions in the sense of having the smallest possible extension over $\mathbb{K}$.

Given a decomposition $f = g(h)$ of a rational function in $\mathbb{K}(x)$, we can write a polynomial system of equations in the coefficients of f, g and h by equating to zero the numerator of $f - g(h)$. The system is linear in the coefficients of g. Therefore, all the coefficients of g and h lie in some algebraic extension of $\mathbb{K}$. Our goal is to find bounds for the degree of the extension $[\mathbb{F} : \mathbb{K}]$ where $\mathbb{F}$ contains, in the sense explained above, all the decompositions of f.

One way to find a bound is by means of a result that relates decomposition and factorization. We state the main definition and theorems here, see [9] for proofs and other details.

Definition 7 *A rational function $f \in \mathbb{K}(x)$ is in* normal form *if* $\deg f_N > \deg f_D$ *and* $f_N(0) = 0$ *(thus* $f_D(0) \neq 0$*).*

Theorem 8

(i) Given $f \in \mathbb{K}(x)$, if $\deg f < |\mathbb{K}|$ *then there exist units u, v such that $u \circ f \circ v$ is in normal form.*

(ii) If $f \in \mathbb{K}(x)$ is in normal form, every decomposition of f is equivalent to one where both components are in normal form.

We will analyze the complexity of finding the units u and v later.

Theorem 9 *Let $f = g(h)$ with f, g, h in normal form. Then h_N divides f_N and h_D divides f_D.*

This result provides the following bound.

Theorem 10 *Let $f \in \mathbb{K}(x)$ and u_1, u_2 be two units in $\mathbb{K}(x)$ such that $g = u_1 \circ f \circ u_2$ is in normal form. Let $\mathbb{F}$ be the splitting field of $\{g_N, g_D\}$. Then any decomposition of f in $\mathbb{K}'(x)$, for any $\mathbb{K}' \supset \mathbb{K}$, is equivalent to a decomposition in $\mathbb{F}(x)$.*

PROOF. By Theorems 8 and 9, every decomposition of g is equivalent to another one, $g = h_1 \circ h_2$, where the numerator and denominator of h_2 divide those of g, thus the coefficients of that component are in $\mathbb{F}$. As the coefficients of h_1 are the solution of a linear system of equations whose coefficients are polynomials in the coefficients of g and h_2, they are also in $\mathbb{F}$. We also have $u_1, u_2 \in \mathbb{K}(x)$, therefore the corresponding decomposition of f lies in the same field. $\square$

This bound, despite being of some interest because its generality and simplicity, is far from optimal. For example, for degree 4 we obtain $[\mathbb{F} : \mathbb{K}] \leq 3! \cdot 3! = 36$. As we will show next, we can use computational algebra techniques, in particular Gröbner bases, to find good bounds for different degrees of f. The following theorem completes Example 5.

Theorem 11 *Let $f \in \mathbb{Q}(x)$ of degree 4. If $f = g(h)$ with $g, h \in \overline{\mathbb{Q}}(x)$, there exists a field $\mathbb{K}$ with $\mathbb{Q} \subset \mathbb{K} \subset \overline{\mathbb{Q}}$ and a unit $u \in \mathbb{K}(x)$ such that $g(u^{-1}), u(h) \in \mathbb{K}(x)$ and $[\mathbb{K} : \mathbb{Q}] \leq 3$.*

PROOF. Without loss of generality we assume

$$f = \frac{x^4 + r_3x^3 + r_2x^2 + r_1x}{s_3x^3 + s_2x^2 + s_1x + 1}, \qquad g = \frac{x^2 + ax}{bx + 1}, \qquad h = \frac{x^2 + cx}{dx + 1}.$$

Then we have the following system of polynomial equations:

$$\begin{aligned}
&ac - r_1 = 0, && 2d + bc - s_1 = 0, \\
&c^2 + cad + a - r_2 = 0, && d^2 + bcd + b - s_2 = 0, \\
&2c + ad - r_3 = 0, && bd - s_3 = 0.
\end{aligned}$$

Let $I \subset \mathbb{C}[r_1, r_2, r_3, s_1, s_2, s_3, a, b, c, d]$ be the ideal generated by these polynomials. Using elimination techniques by means of Gröbner bases (see for example [3]), we find polynomials in I involving $r_1, r_2, r_3, s_1, s_2, s_3$ and each of the variables a, b, c, d:

$$\begin{aligned}
\{\ & a^3 - r_2a^2 + r_1r_3a - r_1^2, \qquad b^3 - s_2b^2 + s_1s_3b - s_3^2, \\
& 2\,c^3 - 2\,r_3c^2 + \left(\tfrac{1}{2}\,r_3^2 + \tfrac{1}{2}\,r_1s_1\right)c - \tfrac{1}{4}\,r_1r_3s_1 + \tfrac{1}{4}\,r_1^2s_3, \\
& 2\,d^3 - 2\,s_1d^2 + \left(\tfrac{1}{2}\,s_1^2 + \tfrac{1}{2}\,r_3s_3\right)d - \tfrac{1}{4}\,r_3s_1s_3 + \tfrac{1}{4}\,r_1s_3^2\ \} \subset I.
\end{aligned}$$

Now it is clear that, given a degree 3 function, the coefficients of its components have degree at most 3 over $\mathbb{Q}$ each. But in fact there is a field of degree 3 that contains all of them:

$$
\begin{aligned}
&ac - r_1 = 0 \quad \Rightarrow \quad c \in \mathbb{Q}(a)\,,\\
&2c + ad - r_3 = 0 \quad \Rightarrow \quad d \in \mathbb{Q}(a, c) = \mathbb{Q}(a)\,,\\
&bd - s_3 = 0 \quad \Rightarrow \quad b \in \mathbb{Q}(d) \subseteq \mathbb{Q}(a)\,.
\end{aligned}
$$

The well–known Extension Theorem (see [3]) may be used to extend the points in the variety defined by $J = I \cap \mathbb{C}[r_1, r_2, r_3, s_1, s_2, s_3]$. This can also be used to study other questions related to the variety, for example the existence of functions with one decomposition in $\mathbb{Q}(x)$ and other in a proper extension of $\mathbb{Q}$. The ideal J determines a variety in $\mathbb{C}^6$ of dimension 4 (in fact, the equations defining I provide a parametrization of the variety), which represents the set of decomposable functions of degree 4 (in normal form). The four polynomials in the different variables showed above allow the successive application of Extension Theorem to prove that each point of J is the image of some point in the parametrization. That is, each point in the variety corresponds to a function of degree 4 that is decomposable in $\mathbb{C}(x)$. From Example 5 we can deduce that, after normalization, not every point of J corresponds to a function that can be decomposed in $\mathbb{Q}(x)$.

Remark 12 *In the polynomial case of degree 4 we have*

$$
f = x^4 + r_3x^3 + r_2x^2 + r_1x\,, \qquad g = x^2 + ax\,, \qquad h = x^2 + cx \in \mathbb{C}(x)\,.
$$

The equations of the ideal $I \subset \mathbb{C}[r_1, r_2, r_3, a, c]$ determined by this are

$$
\begin{aligned}
&I = (\,2c - r_3\,, c^2 + a - r_2\,, ac - r_1\,),\\
&I \cap \mathbb{C}[r_1, r_2, r_3] = \left(\tfrac{1}{8}r_3^3 - \tfrac{1}{2}r_2r_3 + r_1\right).
\end{aligned}
$$

It is clear that, from the initial equations and by Extension Theorem, for each point there exist corresponding values for a, c.

However, if we choose the coefficient field to be $\mathbb{Z}_2$, the ideal is generated by $I = (\,r_3\,,\ c^2 + a + r_2\,,\ ac + r_1\,)$ and the variety is $I \cap \mathbb{C}[r_1, r_2, r_3] = (r_3)$.

We cannot apply Extension Theorem with the generators we have for I; in fact, the polynomial $x^4 + x^2 + x$ is in the variety, but the corresponding equations are $c^2 + a + 1 = 0\,,\ ac + 1 = 0$ which are false for any values $a, c \in \mathbb{Z}_2$, so this polynomial is indecomposable in $\mathbb{Z}_2[x]$.

3 Fixing group and fixed field

In this section we introduce several simple notions from classical Galois theory. Let $\Gamma(\mathbb{K}) = \mathrm{Aut}_{\mathbb{K}}\mathbb{K}(x)$ (we will write simply Γ if there can be no confusion about the field). The elements of $\Gamma(\mathbb{K})$ can be identified with the images of x under the automorphisms, that is, with Möbius transformations (non–constant rational functions of the form $(ax+b)/(cx+d)$), which are also the units of $\mathbb{K}(x)$ under composition.

Definition 13

(i) Let $f \in \mathbb{K}(x)$. We define $G(f) = \{u \in \Gamma(\mathbb{K}) : \ f \circ u = f\}$.

(ii) Let $H < \Gamma(\mathbb{K})$. We define $\mathrm{Fix}(H) = \{f \in \mathbb{K}(x) : \ f \circ u = f \ \forall u \in H\}$.

Example 14

(i) Let $f = x^2 + \dfrac{1}{x^2} \in \mathbb{K}(x)$. Then $G(f) = \left\{x, -x, \dfrac{1}{x}, -\dfrac{1}{x}\right\}$.

(ii) Let $H = \{x, ix, -x, -ix\} \subset \Gamma(\mathbb{C})$. Then $\mathrm{Fix}(H) = \mathbb{C}(x^4)$.

These definitions correspond to the classical Galois correspondences (not bijective in general) between the intermediate fields of an extension and the subgroups of its automorphism group, as the following diagram shows:

$$
\begin{array}{ccc}
\mathbb{K}(x) & \longleftrightarrow & \{id\} \\
| & & | \\
\mathbb{K}(f) & \longrightarrow & G(f) \\
| & & | \\
\mathrm{Fix}(H) & \longleftarrow & H \\
| & & | \\
\mathbb{K} & \longleftrightarrow & \Gamma
\end{array}
$$

Remark 15 *As $\mathbb{K}(f) = \mathbb{K}(f')$ if and only if $f = u \circ f'$ for some unit u, we have that the application $\mathbb{K}(f) \mapsto G(f)$ is well–defined.*

Next, we state several interesting properties of the fixed field and the fixing group.

Theorem 16 *Let H be a subgroup of Γ.*

(i) H is infinite $\Rightarrow \mathrm{Fix}(H) = \mathbb{K}$.

(ii) H is finite $\Rightarrow \mathbb{K} \subsetneq \mathrm{Fix}(H)$, $\mathrm{Fix}(H) \subset \mathbb{K}(x)$ *is a normal extension, and in particular* $\mathrm{Fix}(H) = \mathbb{K}(f)$ *with* $\deg f = |H|$.

PROOF.

(i) It is clear that no non–constant function can be fixed by infinitely many units, as these must fix the roots of the numerator and denominator.

(ii) We will show constructively that there exists f such that $\mathrm{Fix}(H) = \mathbb{K}(f)$ with $\deg f = |H|$. Let $H = \{h_1 = x, \ldots, h_m\}$. Let

$$P(T) = \prod_{i=1}^{m}(T - h_i) \ \in \ \mathbb{K}(x)[T].$$

We will see that $P(T)$ is the minimum polynomial of x over $\mathrm{Fix}(H) \subset \mathbb{K}(x)$. A classical proof of Lüroth's Theorem (see for instance [17]) states that any non–constant coefficient of the minimum polynomial generates $\mathrm{Fix}(H)$, and we are done.

It is obvious that $P(x) = 0$, as x is always in H. It is also clear that $P(T) \in \mathrm{Fix}(H)[T]$, as its coefficients are the symmetric elementary polynomials in $h_1, \ldots, h_m$. The irreducibility is equivalent to the transitivity of the action of the group on itself by multiplication. $\square$

Theorem 17

(i) For any non–constant $f \in \mathbb{K}(x)$, $|G(f)|$ *divides* $\deg f$*. Moreover, for any field* $\mathbb{K}$ *there is a function* $f \in \mathbb{K}(x)$ *such that* $1 < |G(f)| < \deg f$.

(ii) If $|G(f)| = \deg f$ *then* $\mathbb{K}(f) \subseteq \mathbb{K}(x)$ *is normal. Moreover, if the extension* $\mathbb{K}(f) \subseteq \mathbb{K}(x)$ *is separable, then*

$$\mathbb{K}(f) \subseteq \mathbb{K}(x) \textit{ is normal} \quad \Rightarrow \quad |G(f)| = \deg f.$$

(iii) Given a finite subgroup H of Γ, there is a bijection between the subgroups of H and the fields between $\mathrm{Fix}(H)$ *and* $\mathbb{K}(x)$*. Also, if* $\mathrm{Fix}(H) = \mathbb{K}(f)$*, there is a bijection between the right components of f (up to equivalence by units) and the subgroups of H.*

PROOF.

(i) The field $\mathrm{Fix}(G(f))$ is between $\mathbb{K}(f)$ and $\mathbb{K}(x)$, therefore the degree of any generator, which is the same as $|G(f)|$, divides $\deg f$. For the second part, take for example $f = x^2\,(x-1)^2$, which gives $G(f) = \{x, 1-x\}$ in any coefficient field.

(ii) The elements of $G(f)$ are the roots of the minimum polynomial of x over $\mathbb{K}(f)$ that are in $\mathbb{K}(x)$. If there are $\deg\, f$ different roots, as this number equals the degree of the extension we conclude that it is normal.

If $\mathbb{K}(f) \subset \mathbb{K}(x)$ is separable, all the roots of the minimum polynomial of x over $\mathbb{K}(f)$ are different, thus if the extension is normal there are as many roots as the degree of the extension.

(iii) Due to Theorem 16, the extension $\mathrm{Fix}(H) \subset \mathbb{K}(x)$ is normal, and the result is a consequence of the Fundamental Theorem of Galois.

Remark 18 $\mathbb{K}(x)$ *is Galois over* $\mathbb{K}$ *(that is, the only rational functions fixed by* $\Gamma(\mathbb{K})$ *are the constant ones) if and only if* $\mathbb{K}$ *is infinite. Indeed, if* $\mathbb{K}$ *is infinite, for each non–constant function* f *there exists a unit* $x+b$ *with* $b \in \mathbb{K}$ *which does not leave it fixed. On the other hand, if* $\mathbb{K}$ *is finite then* $\Gamma(\mathbb{K})$ *is finite too, an the proof of Theorem 16 provides a non–constant rational function that generates* $\mathrm{Fix}(\Gamma(\mathbb{K}))$.

Algorithms for computing several aspects of Galois theory can be found in [16]. Unfortunately, it is not true in general that $[\mathbb{K}(x) : \mathbb{K}(f)] = |G(f)|$; there is no bijection between intermediate fields and subgroups of the fixing group of a given function. Anyway, we can obtain partial results on decomposability.

Theorem 19 *Let* f *be indecomposable.*

(i) If $\deg\, f$ *is prime, then either* $G(f)$ *is cyclic of order* $\deg\, f$*, or it is trivial.*

(ii) If $\deg\, f$ *is composite, then* $G(f)$ *is trivial.*

PROOF.

(i) If $1 < |G(f)| < \deg\, f$, we have $\mathbb{K}(f) \subsetneq \mathbb{K}(\mathrm{Fix}(G(f))) \subsetneq \mathbb{K}(x)$ and any generator of $\mathbb{K}(\mathrm{Fix}(G(f)))$ is a proper component of f on the right. Therefore, $G(f)$ has order either 1 or $\deg\, f$, and in the latter case, being prime, the group is cyclic.

(ii) Assume $G(f)$ is not trivial. If $|G(f)| < \deg\, f$, we have a contradiction as in (i). If $|G(f)| = \deg\, f$, as it is a composite number, there exists $H \lneq G(f)$ not trivial, and again any generator of $\mathrm{Fix}(H)$ is a proper component of f on the right.

Corollary 20 *If* f *has composite degree and* $G(f)$ *is not trivial,* f *is decomposable.*

Now we present algorithms to efficiently compute fixed fields and fixing groups.

The proof of Theorem 16 provides an algorithm to compute a generator of $\mathrm{Fix}(H)$ from its elements.

Algorithm 1

INPUT*:* $H=\{h_1,\ldots,h_m\}<\Gamma(\mathbb{K})$.
OUTPUT*:* $f\in\mathbb{K}(x)$ *such that* $\mathrm{Fix}(H)=\mathbb{K}(f)$.

A. *Let* $i=1$.
B. *Compute the* i*-th symmetric elementary function* $\sigma_i(h_1,\ldots,h_m)$.
C. *If* $\sigma_i(h_1,\ldots,h_m)\notin\mathbb{K}$*, return* $\sigma_i(h_1,\ldots,h_m)$*. If it is constant, increase* i *and return to* B.

Analysis. The algorithm merely needs computing the product $\prod_{i=1}^{n}(T-h_i)$ using $O(\log n)$ multiplications, so it is efficient both in theory and practice.

Example 21 *Let*

$$H=\left\{\pm x\ ,\pm\frac{1}{x}\ ,\pm\frac{i(x+1)}{x-1}\ ,\pm\frac{i(x-1)}{x+1}\ ,\pm\frac{x+i}{x-i}\ ,\pm\frac{x-i}{x+i}\right\}<\Gamma(\mathbb{C}).$$

Then

$$\begin{aligned}P(T)=T^{12}&-\frac{x^{12}-33x^8-33x^4+1}{x^2(x-1)^2(x+1)^2(x^4+2x^2+1)}\,T^{10}-33\,T^8\\&+2\,\frac{x^{12}-33x^8-33x^4+1}{x^2(x-1)^2(x+1)^2(x^4+2x^2+1)}\,T^6-33\,T^4\\&-\frac{x^{12}-33x^8-33x^4+1}{x^2(x-1)^2(x+1)^2(x^4+2x^2+1)}\,T^2+1\,.\end{aligned}$$

Thus,

$$\mathrm{Fix}(H)=\mathbb{C}\left(\frac{x^{12}-33x^8-33x^4+1}{x^2(x-1)^2(x+1)^2(x^4+2x^2+1)}\right).$$

H is isomorphic to A_4. It is known that A_4 has two complete subgroup chains of different lengths:

$$\{id\}\subset C_2\subset V\subset A_4\,,\qquad \{id\}\subset C_3\subset A_4\,.$$

In our case,

$$\{x\} \subset \{\pm x\} \subset \left\{\pm x, \pm\frac{1}{x}\right\} \subset H\,, \qquad \{x\} \subset \left\{x, \frac{x+i}{x-i}, \frac{i(x+1)}{x-1}\right\} \subset H\,.$$

Applying our algorithm again we obtain the following field chains:

$$\mathbb{C}(f) \ \subset\ \mathbb{C}\left(x^2+\frac{1}{x^2}\right) \ \subset\ \mathbb{C}(x^2) \ \subset\ \mathbb{C}(x)\,,$$

$$\mathbb{C}(f) \ \subset\ \mathbb{C}\left(\frac{-i(t+i)(1+t)t}{(-t+i)(-1+t)}\right) \ \subset\ \mathbb{C}(x)\,.$$

As there is a bijection in this case, the corresponding two decompositions are complete.

In order to compute the fixing group of a function f we can solve the system of polynomial equations obtained from

$$f\left(\frac{ax+b}{cx+d}\right) = f(x).$$

This can be reduced to solving two simpler systems, those given by

$$f(ax+b) = f(x) \qquad \text{and} \qquad f\left(\frac{ax+b}{x+d}\right) = f(x).$$

This method is simple but inefficient; we will describe another method that is faster in practice.

We need to assume that $\mathbb{K}$ has sufficiently many elements. If not, we take an extension of $\mathbb{K}$ and later we check which of the computed elements are in $\Gamma(\mathbb{K})$ by solving simple systems of linear equations.

Theorem 22 *Let $f \in \mathbb{K}(x)$ of degree m in normal form and $u = \dfrac{ax+b}{cx+d}$ such that $f \circ u = f$.*

(i) $a \neq 0$ and $d \neq 0$.

(ii) $f_N(b/d) = 0$.

(iii) If $c = 0$ (that is, we take $u = ax+b$), then $f_N(b) = 0$ and $a^m = 1$.

(iv) If $c \neq 0$ then $f_D(a/c) = 0$.

PROOF.

(i) Suppose $a = 0$. We can assume $u = 1/(cx + d) = (1/x) \circ (cx + d)$. But if we consider $f(1/x)$, its numerator has smaller degree than its denominator. As composing on the right with $cx + d$ does not change those degrees, it is impossible that $f \circ u = f$. Also, as the inverse of u is $\dfrac{dx - b}{-cx + a}$, we have $d \neq 0$.

(ii) Let

$$f = \frac{a_m x^m + \cdots + a_1 x}{b_{m-1} x^{m-1} + \cdots + b_0}.$$

The constant term of the numerator of $f \circ u$ is

$$a_m b^m + a_{m-1} b^{m-1} d + \cdots + a_1 b d^{m-1} = d^m f_N(b/d).$$

As $d \neq 0$ by (i), we have that $f_N(b/d) = 0$. Alternatively, $0 = f(0) = (f \circ u)(0) = f(u(0)) = f(b/d)$.

(iii), (iv) They are similar to the previous item.

We can use this theorem to compute the polynomial and rational elements of $G(f)$ separately.

Algorithm 2

INPUT*:* $f \in \mathbb{K}(x)$.
OUTPUT*:* $G(f) = \{w \in \mathbb{K}(x) : f \circ w = f\}$.

A. *Compute units* u, v *such that* $\overline{f} = u \circ f \circ v$ *is in normal form. Let* $m = \deg f$. *Let* L *be an empty list.*
B. *Compute* $A = \{\alpha \in \mathbb{K} : \alpha^m = 1\}$, $B = \{\beta \in \mathbb{K} : \overline{f}_N(\beta) = 0\}$ *and* $C = \{\gamma \in \mathbb{K} : \overline{f}_D(\gamma) = 0\}$.
C. *For each* $(\alpha, \beta) \in A \times B$, *check if* $\overline{f}(\alpha x + \beta) = \overline{f}(x)$. *In that case add* $ax + b$ *to* L.
D. *For each* $(\beta, \gamma) \in B \times C$, *let* $w = \dfrac{c\gamma\, x + \beta}{c\, x + 1}$. *Compute all values of* c *for which* $\overline{f} \circ w = \overline{f}$. *For each solution, add the corresponding unit to* L.
E. *Let* $L = \{w_1, \ldots, w_k\}$. *Return* $\{v \circ w_i \circ v^{-1} : i = 1, \ldots, k\}$.

Analysis. It is clear that the cost of the algorithm heavily depends on the complexity of the best algorithm to compute the roots of a univariate polynomial in the given field. We analyze the bit complexity when the ground field is the rational number $\mathbb{Q}$. We will use several well–known results about complexity, those can be consulted in the book [7].

In the following, M denotes a multiplication time, so that the product of two polynomials in $\mathbb{K}[x]$ with degree at most m can be computed with at most $M(m)$ arithmetic operations. If $\mathbb{K}$ supports the Fast Fourier Transform, several known algorithms require $O(n \log n \log\log n)$ arithmetic operations. We denote by $l(f)$ the maximum norm of f, that is, $l(f) = \|f\|_\infty = \max |a_i|$ of a polynomial $f = \sum_i a_i x^i \in \mathbb{Z}[x]$.

Polynomials in $f, g \in \mathbb{Z}[x]$ of degree less than m can be multiplied using $O(M(m(l + \log m)))$ bit operations, where $l = \log \max(l(f), l(g))$.

Now, suppose that the given polynomial f is squarefree primitive, then we can compute all its rational roots with an expected number of $T(m, \log l(f))$ bit operations, where $T(m, \log l(f)) =$

$$
\begin{aligned}
&O(m \log(ml(f))(\log^2 \log\log m + (\log\log l(f))^2 \log\log\log l(f)) \\
&+m^2 M(\log(ml(f))).
\end{aligned}
$$

We discuss separately the algorithm steps. Let $f = f_N/f_D$, where $f_N, f_D \in \mathbb{Z}[x]$ and let $l = \log \max(l(f_N), l(g_D))$ and $m = \deg f$.

Step A. Let $u \in \mathbb{Q}(x)$ be a unit such that $g_N/g_D = u(f)$ with $\deg g_N > \deg g_D$. Such a unit always exists:

- If $\deg f_N = \deg f_D$. Let $u = 1/(x - a)$, where $a \in \mathbb{Q}$ verifies $\deg f_N - a \deg f_D < \deg f_N$.
- If $\deg f_N < \deg f_D$, let $u = 1/x$.

Now, let $b \in \mathbb{Z}$ such that $g_D(b) \neq 0$. Then $h_N/h_D = g_N(x+b)/g_D(x+b)$ verifies $h_D(0) \neq 0$ and the rational function $(x - h(0)) \circ h_N/h_D$ is in normal form. Obviously, the complexity in this step is dominated on choosing b. In the worst case, we have to evaluate the integers $0, 1, \ldots, m$ in g_D. Clearly, a complexity bound is $O(M(m^3 l))$.

Step B. Compute the set A can be done on constant time. Now, in order to compute the complexity, we can can suppose, without loss of generality, that $\overline{f_N}$ and $\overline{f_D}$ are squarefree and primitive. Then the bit complexity to compute both set B and set C is $T(m, ml)$.

Step C. A bound for the cardinal of A is 4 and m for the cardinal of B. Then, we need to check $4m$ times if $\overline{f}(\alpha x + \beta) = \overline{f}(x)$ for each each $(\alpha, \beta) \in A \times B$. So, the complexity of this step is bounded by $O(M(m^4 l))$.

Step D. In the worst case the cardinal of $B \times C$ is m^2. This step requires to compute all rational roots of m^2 polynomials $h(x)$ given by the equation:

$$\overline{f} \circ w = \overline{f},$$

for each $(\beta, \gamma) \in B \times C$, where $w = \dfrac{c\gamma\, x + \beta}{c\, x + 1}$. A bound for the degree of $h(x)$ is m^2. The size of the coefficients is bounded by ml, so a bound for total complexity of this step is $m^4 T(m^2, lm^2)$.

Step E. Finally, this step requires substituting at most $2m$ rational functions of degree m and the coefficients size is bounded by lm^3. So, abound for the complexity is $O(M(m^4 l))$.

We can conclude that the complexity of this algorithm is dominated by that of step D, that is, $m^4 T(m^2, lm^2)$. Of course, a worst bound for this is $O(m^8 l^2)$.

The following example illustrates the above algorithm:

Example 23 *Let*

$$f = \frac{(-3x + 1 + x^3)^2}{x(-2x - x^2 + 1 + x^3)(-1 + x)} \in \mathbb{Q}(x).$$

We normalize f: let $u = \dfrac{1}{x - 9/2}$ and $v = \dfrac{1}{x} - 1$, then

$$\overline{f} = u \circ f \circ v = \frac{-4x^6 - 6x^5 + 32x^4 - 34x^3 + 14x^2 - 2x}{27x^5 - 108x^4 + 141x^3 - 81x^2 + 21x - 2}$$

is in normal form.

The roots of the numerator and denominator of $\overline{f}$ in $\mathbb{Q}$ are $\{0, 1, 1/2\}$ and $\{1/3, 2/3\}$ respectively. The only sixth roots of unity in $\mathbb{Q}$ are 1 and -1; as $\operatorname{char} \mathbb{Q} = 0$ *there cannot be elements of the form $x+b$ in $G(\overline{f})$. Thus, there are two polynomial candidates: $-x + 1/3$, $-x + 2/3$. A quick computation reveals that none of them fixes $\overline{f}$.*

Let $w = \dfrac{c\beta\, x + \alpha}{c\, x + 1}$. As $\alpha \in \{0, 1, 1/2\}$ and $\beta \in \{1/3, 2/3\}$, another quick computation shows that

$$G(\overline{f}) = \left\{ \; x, \quad \frac{-x + 1}{-3x + 2}, \quad \frac{-2x + 1}{-3x + 1} \; \right\}$$

and

$$G(f) = v \cdot G(\overline{f}) \cdot v^{-1} = \left\{ x, \quad \frac{1}{1-x}, \quad \frac{x-1}{x} \right\}.$$

From this group we can compute a proper component of f as in the proof of Theorem 19, obtaining $f = g(h)$ with

$$h = \frac{-3\,x + 1 + x^3}{(-1+x)x}, \quad g = \frac{x^2}{x-1}.$$

In the next section we will use these tools to investigate the number of components of a rational function.

4 Ritt's Theorem and number of components

One of the classical Ritt's Theorems (see [13]) describes the relation among the different decomposition chains of a tame polynomial. Essentially, all the decompositions have the same length and are related in a rather simple way.

Definition 24 *A* bidecomposition *is a 4-tuple of polynomials f_1, g_1, f_2, g_2 such that $f_1 \circ g_1 = f_2 \circ g_2$,* deg $f_1 =$ deg g_2 *and* $(\deg f_1, \deg g_1) = 1$.

Theorem 25 (Ritt's First Theorem) *Let $f \in \mathbb{K}[x]$ be tame and*

$$f = g_1 \circ \cdots \circ g_r = h_1 \circ \cdots \circ h_s$$

be two complete decomposition chains of f. Then $r = s$, and the sequences $(\deg g_1, \ldots, \deg g_r)$, $(\deg h_1, \ldots, \deg h_s)$ are permutations of each other. Moreover, there exists a finite chain of complete decompositions

$$f = f_1^{(j)} \circ \cdots \circ f_r^{(j)}, \quad j \in \{1, \ldots, k\},$$

such that

$$f_i^{(1)} = g_i, \quad f_i^{(k)} = h_i, \quad i = 1, \ldots, r,$$

and for each $j < k$, there exists i_j such that the j-th and $(j+1)$-th decomposition differ only in one of these aspects:

(i) $f_{i_j}^{(j)} \circ f_{i_j+1}^{(j)}$ *and* $f_{i_j}^{(j+1)} \circ f_{i_j+1}^{(j+1)}$ *are equivalent.*

(ii) $f^{(j)}_{i_j} \circ f^{(j)}_{i_j+1} = f^{(j+1)}_{i_j} \circ f^{(j+1)}_{i_j+1}$ *is a bidecomposition.*

PROOF. See [13] for $\mathbb{K} = \mathbb{C}$, [5] for characteristic zero fields and [6], [15] for the general case. $\square$

Unlike for polynomials, it is not true that all complete decompositions of a rational function have the same length, as shown in Example 21. The paper [10] presents a detailed study of this problem for non tame polynomial with coefficients over a finite field. The problem for rational functions is strongly related to the open problem of the classes of rational functions which commute with respect to composition, see [14]. In this section we will give some ideas about the relation between complete decompositions and subgroup chains that appear by means of Galois Theory.

Now we present another degree 12 function, this time with coefficients in $\mathbb{Q}$, that has two complete decomposition chains of different length. This function arises in the context of Monstrous Moonshine as a rational relationship between two modular functions (see for example the classical [2] for an overview of this broad topic, or the reference [12], in Spanish, for the computations in which this function appears).

Example 26 *Let $f \in \mathbb{Q}(x)$ be the following degree 12 function:*

$$f = \frac{x^3(x+6)^3(x^2-6\,x+36)^3}{(x-3)^3(x^2+3\,x+9)^3}.$$

f has two decompositions:

$$\begin{aligned} f \;&= g_1 \circ g_2 \circ g_3 \;=\; x^3 \;\circ\; \frac{x(x-12)}{x-3} \;\circ\; \frac{x(x+6)}{x-3} \;= \\ &= h_1 \circ h_2 \;=\; \frac{x^3(x+24)}{x-3} \;\circ\; \frac{x(x^2-6\,x+36)}{x^2+3\,x+9}. \end{aligned}$$

All the components except one have prime degree, hence are indecomposable; the component of degree 4 cannot be written as composition of two components of degree 2.

If we compute the groups for the components on the right in $\mathbb{Q}$ we have:

$$\begin{aligned} G_{\mathbb{Q}}(f) \;&=\; G_{\mathbb{Q}}(g_2 \circ g_3) \;=\; G_{\mathbb{Q}}(g_3) \;=\; \left\{ \frac{3x+18}{x-3},\; x \right\}, \\ G_{\mathbb{Q}}(h_2) \;&=\; \{x\}. \end{aligned}$$

However, in $\mathbb{C}$:

$$G_{\mathbb{C}}(f) = \left\{ \frac{3\alpha_i x + 18\alpha_i}{x-3}, \quad \frac{3\alpha_i x - 18 - 18\alpha_i}{x - 3\alpha_i}, \quad \frac{3\alpha_i x + 18}{x + 3\alpha_i + 3}, \right.$$
$$\left. \frac{3x + 18\alpha_i}{x - 3\alpha_i}, \quad \frac{3x+18}{x-3}, \quad \alpha_i x\,, \; x \right\},$$

$$G_{\mathbb{C}}(g_2 \circ g_3) = \left\{ \frac{3\alpha_i x - 18 - 18\alpha_i}{x - 3\alpha_i}, \quad \frac{3x+18}{x-3}\,, \; x \right\},$$
$$G_{\mathbb{C}}(g_3) = \left\{ \frac{3x+18}{x-3}\,, \; x \right\},$$
$$G_{\mathbb{C}}(h_2) = \left\{ \frac{3\alpha_i x + 18}{x + 3\alpha_i + 3}\,, \; x \right\}$$

where $\alpha_i,\ i = 1, 2$ are the two non-trivial cubic roots of unity.

In order to obtain the function in Example 21, we used Theorem 17, and in particular the existence of a bijection between the subgroups of A_4 and the intermediate fields of a function that generates the corresponding field. The existence of functions with this property has been known for some time, as its construction from any group isomorphic to A_4 is straightforward. On the other hand, the example above is in $\mathbb{Q}(x)$, but there is no bijection between groups and intermediate fields.

In general, there are two main obstructions for this approach. On one hand, there is no bijection between groups and fields in general, as the previous example shows for $\mathbb{Q}$. On the other hand, only some finite groups can be subgroups of $\mathrm{PGL}_2(\mathbb{K})$. The only finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ are C_n, D_n, A_4, S_4 and A_5, see [11]. In fact, this is true for any algebraically closed field of characteristic zero (it suffices that it contains all roots of unity). Among these groups, only A_4 has subgroup chains of different length. This is even worse if we consider smaller fields as the next known result shows:

Theorem 27 *Every finite subgroup of* $\mathrm{PGL}_2(\mathbb{Q})$ *is isomorphic to either* C_n *or* D_n *for some* $n \in \{2, 3, 4, 6\}$.

Indeed these all occur, unfortunately none of them has two subgroup chains of different lengths, so no new functions can be found in this way.

5 Conclusions

In this paper we have presented several counterexamples to the generalization of the first Ritt theorem to rational functions. We also introduced and analyzed several concepts of Galois Theory that we expect to be interesting in providing more structural information in this topic. Also, we show a use of techniques from Computational Algebra results to find bounds for the size of a field that contains all decompositions of a given function; we expect that general properties of Gröbner bases can be applied to this end in order to obtain general bounds.

References

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

[2] J. H. Conway, S. P. Norton, *Monstrous Moonshine*. Bull. Lond. Math. Soc. 11 (1979), 308–339.

[3] D. Cox, J. Little, D. O'Shea, *Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer-Verlag, New York, 1997.

[4] F. Dorey, G. Whaples, *Prime and composite polynomials*. Journal of ALgebra no. 28 (1974), 88–101.

[5] H. T. Engström, *Polynomial substitutions*. Amer. J. Math. 63 (1941), 249–255.

[6] M. Fried, R. Mac Rae, *On the invariance of chains of fields*. Illinois J. Math. 13 (1969), 165–171.

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

[8] J. Gutierrez, *A polynomial decomposition algorithm over factorial domains*. C. R. Math. Rep. Acad. Sci. Canada 13 (1991), no. 2-3, 81–86.

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

[10] J. Gutierrez, D. Sevilla, *On Ritt's decomposition Theorem in the case of finite fields*. Finite Fields and Their Applications. In press, electronic version. 2005.

[11] F. Klein, *The Icosahedron: and the solution of equations of the fifth degree*. Dover, New York, 1956.

[12] J. McKay, D. Sevilla, *Application of univariate rational decomposition to Monstrous Moonshine* (in Spanish). Proceedings of EACA 2004. Pages 289–294.

[13] J. F. Ritt, *Prime and composite polynomials*. Trans. Amer. Math. Soc. 23 (1922), no. 1, 51–66.

[14] J. F. Ritt, *Permutable rational functions.* Trans. Amer. Math. Soc. 25 (1923), no. 3, 399–448.

[15] A. Schinzel, *Polynomials with special regard to reducibility.* Cambridge University Press, New York, 2000.

[16] A. Valibouze, *Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems*, Proc. Applied algebra, algebraic algorithms and error-correcting codes, Paris, 1995. Lecture Notes in Comput. Sci., 948, (1995) pp. 456–468.

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

[18] R. Zippel, *Rational function decomposition.* Proc. ISSAC'91, ACM press (1991), pp. 1–6.