On Decomposition of Tame Polynomials and Rational Functions

Jaime Gutierrez[1], David Sevilla[2]

[1] Faculty of Sciences,
University of Cantabria,
Santander E–39071, Spain
jaime.gutierrez@unican.es
[2] Dpt. of Computer Science and Software Engineering,
Concordia University,
Montréal, QC, H3G 1M8 Canada
dsevilla@cs.concordia.ca

Abstract. In this paper we present algorithmic considerations and theoretical results about the relation between the orders of certain groups associated to the components of a polynomial and the order of the group that corresponds to the polynomial, proving it for arbitrary tame polynomials, and considering the case of rational functions.

1 Introduction

The general functional decomposition problem can be stated as follows: given f in a class of functions, we want to represent f as a composition of two "simpler" functions g and h in the same class, i.e. $f = g \circ h = g(h)$. Although not every function can be decomposed in this manner, when such a decomposition does exist many problems become significantly simpler.

Univariate polynomial decomposition has applications in computer science, computational algebra, and robotics. In fact, computer algebra systems such as AXIOM, MAPLE, MATHEMATICA, and REDUCE support polynomial decomposition for univariate polynomials. For some time, this problem was considered computationally hard: the security of a cryptographic protocol was based on its hardness, see [3]. A polynomial time algorithm is given in [13], requiring $O(ns \log r)$ or $O(n^2)$ field operations, where $n = \deg f$, $r = \deg g$, and $s = \deg h$. It works over any commutative ring in the *tame case*, that is, when the ring contains a multiplicative inverse of r, and assumes that the polynomials involved are monic. Independently, [8] presented a similar algorithm, running in time $O(n^2)$ sequentially and $O(n \log^2 n)$ in parallel. Several papers have been published on different extensions and variations of this problem; see for instance [5],[6], [4], [11] and [7].

In [18] a polynomial time algorithm to decompose a univariate rational function over any field is presented with efficient polynomial factorization. [1] presented two exponential-time algorithms to decompose rational functions, which

are quite efficient in practice. They have been implemented in the MAPLE package CADECOM, which is designed for performing computations in rational function fields; see [9].

In this paper we will focus on certain structural properties of decomposition of polynomials and rational functions in one variable. Namely, for each polynomial or rational function f in one variable, we can consider the group of transformations of the form

$$z \mapsto \frac{az+b}{cz+d} \quad \text{such that} \quad f(z) = f\left(\frac{az+b}{cz+d}\right).$$

The relation between the degree of a rational function and the order of its corresponding group can provide valuable information about the structure of the different decompositions of the function. In particular, the following result appears in [2]:

Theorem 1 ([2]) *Let $p_1, \ldots, p_m \in \mathbb{C}[x]$ be non-constant and $k_1, \ldots, k_m, k$ be the orders of the groups $G(p_1), \ldots, G(p_m), G(p_1 \circ \cdots \circ p_m)$. Then k divides $k_1 \cdots k_m$.*

One of our goal is to generalize this result to a wide class of polynomials, namely the *tame polynomials*, and also consider other generalizations, like the case of rational functions. We think that it can be used to obtain better algorithms for decomposing non tame polynomials, see [6].

2 Polynomial and rational decomposition

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

Definition 1 *Let $\mathbb{K}$ be any field, x a transcendental over $\mathbb{K}$ and $\mathbb{K}(x)$ the field of rational functions in the variable x with coefficients in $\mathbb{K}$. In the set $T = \mathbb{K}(x) \setminus \mathbb{K}$ we define the binary operation of* composition *as*

$$g(x) \circ h(x) = g(h(x)) = g(h).$$

We have that $(T, \circ)$ is a semigroup, the element x being its neutral element.

If $f = g \circ h$, we call this a decomposition *of f 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; the units in $(T, \circ)$ are precisely the elements of the form*

$$\frac{ax+b}{cx+d}, \quad a, b, c, d \in \mathbb{K}, \quad ad - bc \neq 0.$$

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*

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

where the inverse is taken with respect to composition.

Given $f \in T$, we say that it is indecomposable *if it is not a unit and all its decompositions are trivial.*

We define a complete *decomposition of $f \in \mathbb{K}(x)$ 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.*

Definition 2 *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 $\deg a = 0$ *when $a \in \mathbb{K}$.*

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.

Now we introduce some basic results about univariate decomposition, see [1] for more details.

Lemma 1

(i) *For every $f \in T$,* $\deg f = [\mathbb{K}(x) : \mathbb{K}(f)]$.
(ii) $\deg(g \circ h) = \deg g \cdot \deg h$.
(iii) *$f(x)$ is a unit with respect to composition if and only if* $\deg f = 1$, *that is, $f(x) = \dfrac{ax+b}{cx+d}$ with $a, b, c, d \in \mathbb{K}$ and $ad - bc \neq 0$.*
(iv) *Every non–constant element of $\mathbb{K}(x)$ is cancellable on the right with respect to composition. In other words, if $f(x), h(x) \in T$ are such that $f(x) = g(h(x))$ then $g(x)$ is uniquely determined by $f(x)$ and $h(x)$.*

Now we relate decomposition and Field Theory by means of the following extended version of Lüroth's theorem.

Theorem 2 *Let $\mathbb{K}(\mathbf{x}) = \mathbb{K}(x_1, \ldots, x_n)$ be the field of rational functions in the variables $\mathbf{x} = (x_1, \ldots, x_n)$ over an arbitrary field $\mathbb{K}$. If $\mathbb{F}$ is a field of transcendence degree 1 over $\mathbb{K}$ with $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$, then there exists $f \in \mathbb{K}(\mathbf{x})$ such that $\mathbb{F} = \mathbb{K}(f)$. Moreover, if $\mathbb{F}$ contains a non–constant polynomial over $\mathbb{K}$, then there exists a polynomial $f \in \mathbb{K}[\mathbf{x}]$ such that $\mathbb{F} = \mathbb{K}(f)$.*

Proof. For a proof we refer to [16], Theorems 3 and 4, and [14]. Constructive proofs can be found in [15] for $n = 1$, and in [10] for the arbitrary n.

Let $f = g \circ h$. Then $f \in \mathbb{K}(h)$, thus $\mathbb{K}(f) \subset \mathbb{K}(h)$. Also, $\mathbb{K}(f) = \mathbb{K}(h)$ if and only if $f = u \circ h$ for some unit u. This provides the following bijection between the decompositions of a rational function f and the intermediate fields in the extension $\mathbb{K}(f) \subset \mathbb{K}(x)$:

Theorem 3 *Let $f \in \mathbb{K}(x)$. In the set of decompositions of f we have an equivalence relation given by the definition of equivalent decompositions, and we denote as $[(g,h)]$ the class of the decomposition $f = g \circ h$. Then we have the bijection:*

$$\begin{array}{ccc} \{[(g,h)] : f = g(h)\} & \longleftrightarrow & \{\mathbb{F} : \mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(x)\} \\ [(g,h)] & \longleftrightarrow & \mathbb{F} = \mathbb{K}(h). \end{array}$$

Of special interest is the case of f being a polynomial. The following corollary to the second part of Theorem2 shows that, without loss of generality, we can consider only polynomial components.

Corollary 1 *Let f be a polynomial with $f = g \circ h$, where g, h are rational functions. Then there exists a unit u such that*

$$g \circ u, \quad u^{-1} \circ h$$

are polynomials.

Because of this, we only need to consider polynomial decomposition when our original function is a polynomial. In the next section we will define and analyze the notion that will allow us to obtain information about the decompositions of a polynomial.

3 The fixing group of a polynomial

In order to obtain information about the decompositions of a polynomial, we will introduce a concept that comes directly from Galois Theory.

Definition 3 *Let $f \in \mathbb{K}(x)$. The* fixing group *for f is*

$$\Gamma_{\mathbb{K}}(f) = \left\{ \frac{ax+b}{cx+d} : f \circ u = f \right\} < PSL(2, \mathbb{K}).$$

We will drop the subindex when there is no possibility of confusion about the ground field.

This definition corresponds to one of the classical Galois applications between the intermediate fields of an extension and the subgroups of its automorphism group, as the following diagram shows:

$$\begin{array}{ccc} \mathbb{K}(x) & \longleftrightarrow & \{id\} \\ | & & | \\ \mathbb{K}(f) & \longrightarrow & \Gamma_{\mathbb{K}}(f) \\ | & & | \\ \mathbb{K} & \longleftrightarrow & PSL(2, \mathbb{K}) \end{array}$$

Remark 1 *As* $\mathbb{K}(f) = \mathbb{K}(f')$ *if and only if* $f = u \circ f'$ *for some unit* u*, we have that the application* $\mathbb{K}(f) \mapsto \Gamma_{\mathbb{K}}(f)$ *is well–defined.*

Next, we state several interesting properties of the fixing group, see [12] for details.

Theorem 4

(i) *Given* $f \in \mathbb{K}(x) \setminus \mathbb{K}$, $|\Gamma_{\mathbb{K}}(f)|$ *divides* $\deg f$*. Moreover, for any field* $\mathbb{K}$ *there is always a function* $f \in \mathbb{K}(x)$ *such that* $1 < |\Gamma_{\mathbb{K}}(f)| < \deg f$*, for example for* $f = x^2 (x-1)^2$ *we have* $\Gamma_{\mathbb{K}}(f)$=$\{x,1\text{-}x\}$ *for any* $\mathbb{K}$*.*

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

$$\mathbb{K}(f) \subseteq \mathbb{K}(x) \text{ is normal} \Rightarrow |\Gamma_{\mathbb{K}}(f)| = \deg f.$$

4 Uniqueness of intermediate fields of the same degree

First, we will define the class of polynomials on which we will work.

Definition 4 *A polynomial* $f \in \mathbb{K}[x]$ *is* tame *when* $\operatorname{char} \mathbb{K}$ *does not divide* $\deg f$*.*

The following result shows a nice property of tame polynomials.

Theorem 5 *Let* $f \in \mathbb{K}[x]$ *be tame and* $f = g_1 \circ h_1 = g_2 \circ h_2$ *such that* $\deg h_1 = \deg h_2$*. Then there exists a polynomial unit* u *such that* $h_1 = u \circ h_2$*.*

Proof. See [7].

Due to the equivalence given by Theorem 3, the previous theorem is equivalent to the uniqueness of intermediate fields of the same degree; that is, if $\mathbb{K}(h_1)$, $\mathbb{K}(h_2)$ are fields between $K(f)$ and $\mathbb{K}(x)$ and $\deg h_1 = \deg h_2$, then $\mathbb{K}(h_1) = \mathbb{K}(h_2)$.

This is not true if we drop the tameness hypothesis.

Example 1 ([17]) *Let* $\mathbb{K} = \mathbb{F}_2$, $\alpha^2 - \alpha + 1 = 0$ *with* $\alpha \in \mathbb{F}_4$*. We have that*

$$x^4 + x^2 + x = (x^2 + \alpha x)^2 + \alpha^{-1}(x^2 + \alpha x).$$

In the case of rational functions, the result is also false.

Example 2 ([1]) *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 ω *is a non-real cubic root of unity in* $\mathbb{Q}$*.* f *is indecomposable in* $\mathbb{Q}(x)$*. However,* $f = f_1 \circ f_2$ *where*

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

Example 3 *Let*

$$f = x^2 + \frac{1}{x^2}.$$

This function has two different decompositions that are not equivalent:

$$f = \frac{1}{x} \circ x^2 = (x^2 - 2) \circ \frac{1}{x}.$$

5 Main result

In relation to the existence of these fields we will discuss the generalization of the following result:

Theorem 6 ([2]) *Let $p_1, \ldots, p_m \in \mathbb{C}[x]$ be non-constant and $k_1, \ldots, k_m, k$ be the orders of the groups $\Gamma(p_1), \ldots, \Gamma(p_m), \Gamma(p_1 \circ \cdots \circ p_m)$. Then k divides $k_1 \cdots k_m$.*

We try to generalize this to polynomials with coefficients in any field. First we study the fixing groups of these polynomials.

Theorem 7 *Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[x]$ a tame polynomial. Then $\Gamma(f)$ is cyclic.*

Proof. First we prove that there are no elements of the form $x + b$ in $\Gamma(f)$ with $b \neq 0$. Let $H = \{x + b : b \in \mathbb{K}, f(x + b) = f(x)\} < \Gamma(f)$.

If char $\mathbb{K} = p > 0$, any element $x + b \in H$ with $b \neq 0$ has order p, so the order of H is divisible by p. But the order of H divides deg f, therefore H is a trivial group. If char $\mathbb{K} = 0$, no elements of the form $x + b$ with $b \neq 0$ have finite order.

Let $a, b, c \in \mathbb{K}$ be such that $ax+b,\ ax+c \in \Gamma(f)$. Then $(ax+b)\circ(ax+c)^{-1} = x + c - b$, thus $b = c$. Therefore, $B = \{a \in \mathbb{K}^* : \exists b \,|\, ax + b \in \Gamma(f)\}$, a subgroup of the multiplicative group $\mathbb{K}^*$, has the same order as $\Gamma(f)$. But B is cyclic, thus there exists $a_0 \in \mathbb{K}^*$ such that $B =< a_0 >$. Given the corresponding $a_0x + b_0 \in \Gamma(f)$, it is clear that every element of $\Gamma(f)$ is a power of it, therefore $\Gamma(f)$ is cyclic.

We can now generalize Theorem 6 to the case of tame polynomials:

Theorem 8 *Let $\mathbb{K}$ be any field and $p_1, \ldots, p_m \in \mathbb{K}[x]$ be tame. Let $k_1, \ldots, k_m, k$ be the orders of $\Gamma(p_1), \ldots, \Gamma(p_m), \Gamma(p_1 \circ \cdots \circ p_m)$. Then k divides $k_1 \cdots k_m$.*

Proof. It suffices to take $m = 2$ and then use induction. Let γ be a generator of the cyclic group $\Gamma(p_1 \circ p_2)$. As $p_1 \circ p_2 = (p_1 \circ p_2) \circ \gamma = p_1 \circ (p_2 \circ \gamma)$, by Theorem 5 there exists a unit η such that $p_2 \circ \gamma = \eta \circ p_2$. Then $p_1 \circ p_2 = p_1 \circ p_2 \circ \gamma = p_1 \circ \eta \circ p_2$, therefore $p_1 \circ \eta = p_1$. That is, $\eta \in \Gamma(p_1)$ and its order l_1 divides k_1.

On one hand, $p_2 \circ \gamma = \eta \circ p_2$ implies $p_2 \circ \gamma^r = \eta^r \circ p_2$ for each integer r. Taking $r = k$, we have $\eta^k = x$, thus l_1 divides k. On the other hand, taking $r = l_1$ we have $\gamma^{l_1} \in \Gamma(p_2)$, that has order $l_2 = k/l_1$. Therefore, as $l_1 | k_1, l_2 | k_2$ y $l_1 l_2 = k$, we have $k | k_1 k_2$.

6 Generalizations and future work

In the rational case, as the uniqueness of fields of the same degree is not true in general as proved by Examples 2 and 3, we can think that this theorem cannot be generalized. This is indeed the case, as the next example shows.

Example 4 *Let*

$$f = \frac{-1 + 33x^4 + 33x^8 - x^{12}}{x^2 - 2x^6 + x^{10}}.$$

We have that

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

The element $i(x+1)/(x-1)$ has order 3, and a function that is fixed by it is

$$h = \frac{x^3 + (x-1)x + 1 - i}{(x-1)(x-i)}.$$

The field $\mathbb{C}(h)$ is not left invariant by every element of $\Gamma_{\mathbb{C}}(f)$, only by the three elements in the subgroup (as they leave the generator fixed). For example it is easy to check that

$$h \circ (-x) \notin \mathbb{C}(h).$$

Still, the following conjecture can be posed even if the prove is not valid in this case.

Conjecture 1 *Theorem 8 is true for every rational function whose degree is not a multiple of the characteristic of the field.*

A different direction that may allow for some generalization is given by the relation between the degrees of the components for tame polynomials:

Theorem 9 ([17]) *If $\mathbb{K}(f) \cap \mathbb{K}(g)$ contains a polynomial h such that* $\deg h \not\equiv 0 \bmod \operatorname{char} \mathbb{K}$*, then*

$$[\mathbb{K}(f) : \mathbb{K}(f) \cap \mathbb{K}(g)] = \frac{\operatorname{lcm}(\deg f, \deg g)}{\deg f},$$

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

Because of this, it is possible to consider that, as in Theorem 8 not only k divides $k_1 k_2$, but also $\gcd(k_1, k_2)$. The following trivial example shows that this is not true in general:

Example 5 *The function $x^4 = x^2 \circ x^2$ does not satisfy the above statement, since $4 \nmid 2$.*

In any case, we consider that it is of interest to study the classes of polynomials and rational functions for which these statements hold.

Acknowledgment. This work is partially supported by Spanish Ministry of Science grant MTM2004-07086.

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. A. F. Beardon, T. W. Ng, *On Ritt's factorization of polynomials*. J. London Math. Soc. (2) 62 (2000), no. 1, 127–138.
3. Cade, J.(1985). A new public-key cipher which allows signatures. *Proc. 2nd SIAM Conf on Appl. Linear Algebra*, Raleigh NC.
4. Casperson, D., Ford, D., MacKay, J. (1996). An ideal decomposition Algorithm. *J. Symbolic Computation* 21, no. 2, 133–137.
5. J. von zur Gathen, *Functional decomposition of polynomials: the tame case*. J. Symbolic Computation, **9**,(1990), 281-299.
6. J, von zur Gathen, *Functional decomposition of polynomials: the wild case*. J. Symbolic Computation, **10**,(1990), 437–452.
7. J. Gutierrez, *A polynomial decomposition algorithm over factorial domains*. C. R. Math. Rep. Acad. Sci. Canada 13 (1991), no. 2-3, 81–86.
8. Gutierrez, J., Recio, T., Ruiz de Velasco, C. (1989). A polynomial decomposition algorithm of almost quadratic complexity. *Proc. AAECC-6/88*. L. N. Computer Science 357, 471–476.
9. Gutierrez, J., Rubio, R. (2000). CADECOM: Computer Algebra software for functional DECOMposition. *Proceedings of the Second Workshop on Computer Algebra in Scientific Computing*, V. G. Ganzha, E. W. Mayr, E. V. Vorozhtsov, editors, Samarkand, Uzbekistan, Springer–Verlag, 233–248.
10. J. Gutierrez, R. Rubio, D. Sevilla, *On Multivariate Rational Function Decomposition* J. Symbolic Comput. 33 (2002), 545–562.
11. Gutiérrez, J., Rubio, R., Gathen von zur, J.: *Multivariate Polynomial decomposition*. Applicable Algebra in Engineering, Communication and Computing, **14 (1)** 11–31. (2003).
12. J. Gutierrez, D. Sevilla, *On Ritt's decomposition Theorem in the case of finite fields*, *Finite Fields and Their Applications* . In press doi:10.1016/j.ffa.2005.08.004. Available online.
13. D. Kozen, S. Landau, *Polynomial decomposition algorithms*. J. Symbolic Computation. **7** (1989), 445–456.
14. M. Nagata, *T*heory of Commutative Fields, Translations of Mathematical Monographs, Amer. Math. Soc., **125** (1993).
15. E. Netto, *Ünber einen Lüroth-Gordaschen Satz*. Math. Ann. 9 (1895), 310–318.
16. A. Schinzel: *Selected Topics on Polynomials*. Ann Arbor, University Michigan Press, 1982.
17. A. Schinzel, *Polynomials with special regard to reducibility*. Cambridge University Press, New York, 2000.
18. Zippel, R. (1991). Rational Function Decomposition. *Proc. ISSAC-91*. ACM press, 1–6.