Dijana KRESO

Rational function decomposition and Diophantine equations

PHD THESIS

written to obtain the academic degree of a Doctor of Engineering Sciences

Doctoral studies of Engineering
at the doctoral school "Mathematics and Scientific Computing"

Graz University of Technology

Graz University of Technology

Supervisor:
Ao.Univ.-Prof. Dipl.-Ing. Dr.techn. Robert Tichy

Institute of Analysis and Computational Number Theory (Math A)

Graz, January 2014

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

....

(date) (signature)

Contents

Acknowledgements

First and foremost, I would like to thank my advisor Professor Robert Tichy for his patient guidance and support throughout my doctoral studies.

My special thanks goes to Professor Michael Zieve for his tireless and patient help. I'm very grateful that I have had the opportunity to work with him.

My grateful thanks are also extended to my co-authors András Baszó, Zrinka Franušić, Florian Luca, Ákos Pintér and Csaba Rakaczki. I thank them greatly for sharing their time and ideas with me. Another thanks goes to Professor Ákos Pintér for hosting me several times at University of Debrecen. I thank him for his kindness and hospitality.

I further thank Professor Andrej Dujella for his constant support and encouragement. Advice given by him has always been greatly appreciated.

Special thanks goes to my colleague Daniel Smertnig for always finding time to read my materials and for helping me find answers to my math problems.

I thank many people who have helped me throughout the completion of this thesis. I particularly thank Christian Elsholtz, Clemens Fuchs, Alfred Geroldinger and Thomas Stoll.

I further thank the Austrian Science Fund (FWF) for funding the doctoral school *Discrete Mathematics*, which I am associated to. Thanks to them I had the opportunity to travel a lot, meet other mathematicians and expand my math horizons, which has been of great value.

My special thanks are extended to my colleagues for making my time in Graz joyful and pleasant.

Lastly, I thank my family and friends for their constant encouragement and belief in me.

Preface

This PhD thesis contains a collection of papers of the author. Three of these are already published. All the details can be found in the Publication List following this preface. The fourth paper *Invariants of functional decomposition of rational functions* is in preparation and will soon be submitted for publication.

The structure of this thesis is as follows. After the introduction, there are four chapters and each corresponds to one publication. At the beginning of each of those chapters, more information about the publication can be found. The last chapter contains a publication that is quite unrelated to the main topic of this thesis. This publication is incorporated into the thesis, since it was published during the doctoral studies of the author.

Publication List

[i] A. Bazsó, D. Kreso, F. Luca, and Á. Pintér, *On equal values of power sums of arithmetic progressions*, Glas. Mat. Ser III **47(67)** (2012), 253–263.

[ii] Z. Franušić and D. Kreso, *Non-extensibility of the pair* $\{1, 3\}$ *to a Diophantine quintuple in* $\mathbb{Z}[\sqrt{-2}]$, J. of Comb. Number Theory **3** (2011), 151–165.

[iii] D. Kreso and Cs. Rakaczki, *Diophantine equations with Euler polynomials*, Acta Arith. **161** (2013), 267–281.

[iv] D. Kreso and M.E. Zieve, *Invariants of functional decomposition of rational functions*, in preparation.

Chapter 1

Introduction

In 1920's, the creators of modern iteration theory Fatou, Julia and Ritt made extensive studies of commuting polynomials, that is, $f, g \in \mathbb{C}[x]$ that satisfy $f \circ g = g \circ f$. The Julia set arose from such studies, as a consequence of a result of Julia that two commuting polynomials have the same Julia set. Ritt [**85**] determined all commuting rational functions. Ritt [**84**] further studied more general functional equation $f_1 \circ f_2 \circ \cdots \circ f_m = g_1 \circ g_2 \circ \cdots \circ g_n$ in non-constant complex polynomials. This led him to study possible ways of writing a complex polynomial as a functional composition of polynomials of lower degree. A polynomial $f \in \mathbb{C}[x]$ with $\deg f > 1$ is called *indecomposable* if it cannot be written as a composition $f(x) = g(h(x))$ with $g, h \in \mathbb{C}[x]$ and $\deg g, \deg h > 1$. It follows by induction that any polynomial $f(x)$ with $\deg f > 1$ can be written as a composition of indecomposable polynomials – such an expression of $f(x)$ is said to be a *complete decomposition* of $f(x)$. Ritt proved that one can obtain any complete decomposition of $f(x)$ from any other through finitely many steps, where each step consists of replacing two adjacent indecomposable polynomials by two others with the same composition. This result is known in literature as Ritt's first theorem. Ritt then solved the equation $a \circ b = c \circ d$ in indecomposable $a, b, c, d \in \mathbb{C}[x]$. The trivial solutions are $a \circ b = (a \circ \ell) \circ (\ell^{\langle -1 \rangle} \circ b)$ for any linear $\ell \in \mathbb{C}[x]$, where $\ell^{\langle -1 \rangle}(x)$ denotes the inverse of $\ell(x)$ with respect to functional composition. Ritt proved that, up to such insertions of linear polynomials, the only nontrivial solutions are $x^n \circ x^m f(x^n) = x^m f(x)^n \circ x^n$ and $T_n(x) \circ T_m(x) = T_m(x) \circ T_n(x)$, where $f(x) \in \mathbb{C}[x]$, n, m are positive integers and $T_n(X)$ is the n-th Chebychev polynomial of the first kind (defined via identity $T_n(\cos(\alpha)) = \cos(n\alpha)$). Ritt further generalized this result by finding all solutions of the equation $a \circ b = c \circ d$, which satisfy $\deg(a) = \deg(d)$ and $\gcd(\deg(a), \deg(c)) = 1$ (note that the solutions of $a \circ b = c \circ d$ in indecomposables satisfy these conditions). This result is known in literature as Ritt's second

theorem. Simplified and modernized versions of Ritt's proofs together with a complete exposition of related results can be found in [**96**].

In his proofs, Ritt used the language of Riemann surfaces. It was therefore somewhat surprising that his results could be extended to polynomials over fields other than the complex numbers. In 1941 and 1942, Engstrom [**36**] and Levi [**65**], using different (algebraic) methods, showed that the great portion of Ritt's results (these did not include Ritt's second theorem in full generality) hold over an arbitrary field of characteristic zero. In 1969, Fried and McRae [**45**] proved that these results remain valid over fields of positive characteristic as well, provided characteristic of the field does not divide the degree of the polynomial under consideration. In 1974, Dorey and Whaples [**25**] noticed that Ritt's proofs do not make essential use of the topological structure of Riemann surfaces; they followed Ritt's ideas and gave group-theoretic proof of Ritt's first theorem and valuation-theoretic proof of Ritt's second theorem (but under simplifying assumption that $a, b, c, d \in \mathbb{C}[x]$ in $a \circ b = c \circ d$ are indecomposable). In the same paper Dorey and Whaples further provided an example of a polynomial $f(x)$ with coefficients in a field K satisfying $\mathrm{char}(K) \mid \deg f$, which has two complete decompositions consisting of a different number of indecomposables. In 1993, Zannier [**94**] proved an analogue of Ritt's second theorem in fields of positive characteristic. Alternative proofs of the aforementioned results were further given by Fried [**43**], Schinzel [**88, 89**], Tortratt [**93**], Bilu and Tichy [**13**] and others. These results have many applications to various areas of mathematics that include:

1. Bilu and Tichy's [**13**] classification of all $f, g \in \mathbb{Q}[x]$ such that the equation $f(x) = g(y)$ has infinitely many integer solutions,
2 Pakovich's classification [**75**] of $f, g \in \mathbb{C}[x]$ and compact subsets $A, B \subseteq \mathbb{C}$ such that $f^{-1}(A) = g^{-1}(B)$,
3 Beal, Wetherell and Zieve's [**7**] description of $K[f] \cap K[g]$ and $K(f) \cap K(g)$ for $f, g \in K[x]$, where K is a field of characteristic zero,
4 Ghioca, Tucker and Zieve's [**48**] classification of complex polynomials that have orbits with infinite intersection,
5 Medvedev and Scanlon's [**68**] description of the affine varieties that are invariant under a coordinatewise polynomial action.

We come back to Bilu and Tichy's classification later in this introduction. Chapters 3 and 4 concern the applications of Bilu and Tichy's classificiation. In what follows, we study in more detail polynomial decomposition questions with special focus on invariants of complete decomposition, as well as rational function analogues of these results; this is the main topic of Chapter 2.

1. Invariants of rational function decomposition

As we have seen, all the solutions of the equation $a \circ b = c \circ d$ in indecomposable $a, b, c, d \in \mathbb{C}[x]$ satisfy either $\deg a = \deg c$ and $\deg b = \deg d$, or $\deg a = \deg d$ and $\deg b = \deg c$. From Ritt's first theorem it follows therefore that any two complete decomposition of $f \in \mathbb{C}[x]$ consist of the same number of indecomposable polynomials and that the sequences of degrees of indecomposable polynomials in any two complete decompositions of $f(x)$ are the same, up to permutation. In 2000, Beardon and Ng [**8**] presented another invariant of polynomial decomposition. Writing $\Gamma(f)$ for the set of linear $\ell \in \mathbb{C}[x]$ such that $f \circ \ell = f$ and $\gamma(f)$ for the size of the set $\Gamma(f)$, Beardon and Ng showed that if $f = f_1 \circ f_2 \circ \cdots f_n$ is a complete decomposition of $f \in \mathbb{C}[x]$, then the sequence $(\gamma(f_1), \gamma(f_2), \ldots, \gamma(f_n))$ is uniquely determined by $f(x)$, up to permutation. Beardon and Ng further showed that if $f = f_1 \circ f_2 \circ \cdots f_n$ for $f, f_1, \ldots, f_n \in \mathbb{C}[x]$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$. Gutierrez and Sevilla [**55**] extended the latter result to the case when $f, f_1, \ldots, f_n \in K[x]$, where K is a field such that $\mathrm{char}(K) \nmid \deg f$.

Very recently, Zieve and Müller [**96**] presented a new invariant which generalizes both Ritt's degree invariant and the invariant of Beardon and Ng. To state it, we need to introduce the notion of monodromy group.

Definition 1. Let K be a field. Given a $f \in K(x)\backslash K$ the *monodromy group* $\mathrm{Mon}(f)$ is the Galois group of (the numerator) of $f(x) - t$ over $K(t)$, where t is transcendental over K, viewed as a group of permutations of the roots of $f(x) - t$.

The importance of the monodromy group when analyzing various questions about polynomials was exhibited by Fried in [**42, 41**]. More details on the importance of the monodromy group when analyzing decomposition questions, will be given later in this introduction. Zieve and Müller [**96**] showed that if $f = f_1 \circ f_2 \circ \cdots f_n$ is a complete decomposition of $f(x) \in \mathbb{C}[x]$, then the sequence of permutation groups $(\mathrm{Mon}(f_1), \mathrm{Mon}(f_2), \ldots, \mathrm{Mon}(f_n))$ is uniquely determined by $f(x)$, up to permutation. Since $\mathrm{Mon}(f_i)$ acts on the set of size $\deg f_i$, it follows that the monodromy invariant generalizes Ritt's degree invariant. In [**96**], it is proved that for indecomposable f_i, $\gamma(f_i) = 1$ unless $\mathrm{Mon}(f_i)$ is cyclic, in which case $\gamma(f_i) = |\mathrm{Mon}(f_i)| = \deg f_i$; hence the monodromy invariant generalizes the invariant of Beardon and Ng as well.

In Chapter 2 we give a common generalization of these results for rational functions over an arbitrary field that satisfy certain conditions on the monodromy group. In so doing, we recover most of the known results on invariants of polynomial decomposition and present several new ones. In our proofs, we follow the Galois-theoretic approach developed by Ritt [**84**], which we recall in

the following section. The approach we take clarifies why these results are true in some settings and not in others.

Methods and results. We use the following notation throughout this section: K is an arbitrary field and $f \in K(x)$. We define a decomposition of $f(x)$ to be an expression $f = f_1 \circ \cdots \circ f_n$ with $f_i \in K(x)$ and $\deg f_i > 1$. We say that $f \in K(x)$ with $\deg f > 1$ is *indecomposable* (over K) if it has no decomposition of length $n \geq 2$. *Complete decomposition* of $f(x)$ (over K) is an expression of $f(x)$ as the composition of indecomposable rational functions in $K(x)$. Write $f(X) = f_N(X)/f_D(X)$, where $f_N, f_D \in K[X]$ are relatively prime and recall that then $\deg f$ is defined as maximal between $\deg f_N$ and $\deg f_D$.

The following result of Lüroth, provides a dictionary between decompositions of $f(x)$ and fields between $K(f(x))$ and $K(x)$.

THEOREM 1 (Lüroth's theorem). *Let K and L be fields such that $K \subseteq L \subseteq K(x)$, where x is transcendental over K. Then $L = K(h(x))$ for some $h(x) \in K(x)$.*

If $f = g \circ h$, then $K(h(x))$ clearly lies between $K(f(x))$ and $K(x)$. For a non-constant $f \in K(x)$, Lüroth's theorem implies that any field L such that $K(f(x)) \subseteq L \subseteq K(x)$ must be of the form $L = K(h(x))$ for some $h(x) \in K(x)$. Since $f(x) \in K(h(x))$ it follows that $f = g \circ h$ for some $g(x) \in K(x)$. We do not have a bijection here since the generator of an intermediate field of $K(x)/K(f(x))$ is not uniquely determined. However, for non-constant $h_1, h_2 \in K(x)$, it is easy to see that $K(h_1(x)) = K(h_2(x))$ if and only if $h_1 = \mu \circ h_2$ for some degree-one $\mu(x) \in K(x)$. This motivates the following definition.

DEFINITION 2. For $f \in K(x)$, we say that two decompositions $f = f_1 \circ \cdots \circ f_n$ and $f = g_1 \circ \cdots \circ g_m$ of $f(x)$ are *equivalent* if $n = m$ and there are degree-one $\mu_0, \ldots, \mu_n \in K(x)$, with $\mu_0 = \mu_n = x$, such that $g_i = \mu_{i-1} \circ f_i \circ \mu_i^{\langle -1 \rangle}$ for $1 \leq i \leq n$, where $\mu^{\langle -1 \rangle}$ denotes the inverse of μ with respect to functional composition.

Hence, the class of decompositions of $f(x)$ that are equivalent to the decomposition $f = f_1 \circ \cdots \circ f_n$, corresponds to the chain of fields $K(x) \supset K(f_n(x)) \supset K(f_{n-1} \circ f_n(x)) \supset \cdots \supset K(f_1 \circ \cdots \circ f_n(x)) = K(f(x))$. We are of course interested in the possible ways rational functions decompose up to equivalence, so we may say that a complete decomposition of $f(x)$ corresponds to the chain of fields between $K(f(x))$ and $K(x)$. Note that if $f'(x) \neq 0$, the extension $K(x)/K(f(x))$ is separable. If so and if L is the Galois closure of $K(x)/K(f(x))$, then fields between $K(f(x))$ and $K(x)$ correspond to groups between associated Galois groups – $\mathrm{Mon}(f) = \mathrm{Gal}(L/K(f(x)))$ and the point stabilizer in $\mathrm{Mon}(f)$, that is $\mathrm{Gal}(L/K(x))$. Note that a complete decomposition of $f(x)$ corresponds

to the decreasing maximal chain of groups between $\mathrm{Mon}(f)$ and the point stabilizer in $\mathrm{Mon}(f)$. Further note that $f(x)$ is indecomposable if and only if the point stabilizer is a maximal subgroup of $\mathrm{Mon}(f)$. It is well known that the point stabilizer is a maximal subgroup of the permutation group if and only if this group is primitive (it does not preserve a non-trivial partition of the underlying set). Hence, $f(x)$ is indecomposable if and only if $\mathrm{Mon}(f)$ is a primitive permutation group. This was first observed in [**45**]. We remark that Müller [**71**] classified the monodromy groups of indecomposable complex polynomials using the classification of finite simple groups.

There are no known analogues of Ritt's results for rational functions. Ritt [**85, 86**] first studied this question and was aware of the fact that there exist complex rational functions with two complete decompositions of different length; he noticed that the fact that A_4 has two maximal chains of subgroups of different length, namely $1 < C_2 < V_4 < A_4$ and $1 < C_3 < A_4$, implies the following counterexample, that was recently reproduced in [**54**].

Example 1. Let

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

Then

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

To see that $g_1(x), g_2(x), g_3(x)$ and $h_2(x)$ are indeed indecomposable rational functions, note that every rational function of prime degree is indecomposable (since if rational functions f, g, h satisfy $f = g \circ h$, then $\deg f = \deg g \cdot \deg h$). It can be directly verified that $h_1(x)$ can not be written as a functional composition of two rational functions of degree 2, which is the only possibility for $h_1(x)$ to be indecomposable since $\deg h_1 = 4$.

Further families of counterexamples to the rational function analogues of Ritt's results can be found in [**67**]. It is further noted there that all known counterexamples fall into certain classes, which suggests that there might be a precise description of all such counterexamples, but that current techniques seem to be insufficient for proving such results. In general, very few results on rational function decomposition exist. Among best ones is still already mentioned Ritt's result on commuting rational functions [**85**]. We further mention [**95**], where analogues of Ritt's results are shown for Laurent polynomials.

We now quickly explain why Ritt's method for polynomials does not apply to rational functions. Ritt [**84**] observed that for $f \in \mathbb{C}[x]$ there exists a transitive

cyclic subgroup of $\mathrm{Mon}(f)$, namely the inertia group at any infinite place of the Galois closure of $\mathbb{C}(x)/\mathbb{C}(f(x))$, and that the questions about decompositions of $f(x)$ can be translated into questions about subgroups of this cyclic group. The same holds if $f \in K[x]$, where K is a field such that $\mathrm{char}(K) \nmid \deg f$; as already mentioned, the analogues of Ritt's results are known in this case, see [**45**]. A transitive cyclic subgroup of $\mathrm{Mon}(f)$ does not need to exist when $f \in K[x]$ with $\mathrm{char}(K) \mid \deg f$, nor when $f \in K(x)$ is arbitrary. As already mentioned, in both cases there exist examples with two complete decompositions of different length, see [**25, 55, 86**].

Several appealing results can be shown for $f \in K(x)$ such that $\mathrm{Mon}(f)$ has a transitive quasi-Hamiltonian subgroup. A group A is said to be quasi-Hamiltonian if the product of any two subgroups of A is a group; the structure of such groups was described by Iwasawa [**58**] in 1941. As we have seen, the study of decompositions of $f(x)$ reduces to the study of groups between $\mathrm{Mon}(f)$ and the point stabilizer Stab_x in $\mathrm{Mon}(f)$. If A is a transitive subgroup of $\mathrm{Mon}(f)$, then clearly $\mathrm{Mon}(f) = A\mathrm{Stab}_x$. Then the study of groups between Stab_x and $\mathrm{Mon}(f)$ reduces to the study of subgroups of A. If A is further quasi-Hamiltonian, then we can prove the following generalization of Ritt's first theorem. To state our theorem precisely, we first introduce the following definition.

Definition 3. We call two complete decompositions $f = f_1 \circ \cdots \circ f_n$ and $f = g_1 \circ \cdots \circ g_n$ Ritt neighbors if there exists i, with $1 \leq i < n$, such that $f_j = g_j$ for all $j \notin \{i, i+1\}$ and $f_i \circ f_{i+1} = g_i \circ g_{i+1}$.

Theorem 2. *Let K be a field and $f \in K(x)$ such that $f'(x) \neq 0$. If the monodromy group of $f(x)$ has a transitive quasi-Hamiltonian subgroup, then any complete decomposition of $f(x)$ can be obtained from any other complete decomposition of $f(x)$ through finitely many steps, where in each step we replace a complete decomposition of $f(x)$ by a Ritt neighbor.*

We further study the solutions of $f = a \circ b = c \circ d$, in indecomposable rational functions $a, b, c, d \in K(x)$ under the same assumption on $f(x)$ as in Theorem 2. We get that the degrees of a and b are the same as those of c and d, but possibly in reversed order. We do not know whether, under the same condition on $f(x)$, one has that $\mathrm{Mon}(a)$ and $\mathrm{Mon}(c)$ are isomorphic as permutation groups to $\mathrm{Mon}(b)$ and $\mathrm{Mon}(d)$ (again possibly in reversed order). Despite of a deep computer search, we did not find any counterexamples. We prove this result under a stronger condition on $f(x)$. If $f'(x) \neq 0$ and the monodromy group of $f(x)$ has a transitive quasi-Hamiltonian subgroup A such that any nontrivial subgroup of A contains a nontrivial normal subgroup of A, then the result follows. This clearly holds if $\mathrm{Mon}(f)$ has a transitive Dedekind subgroup. Recall that a group A is called Dedekind if every subgroup of A is normal. Under this stronger

assumption on f, we also get that if $f = f_1 \circ f_2 \circ \cdots f_n$ for $f_1, \ldots, f_n \in K(x)$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$, where $\gamma(f) = |\{\mu \in K(x) : f(\mu(x)) = f(x)\}|$. In this way we generalize and give new proofs of aforementioned results of Beardon–Ng [**8**] and Gutierrez–Sevilla [**55**].

The following conjecture was posed by Gutierrez and Sevilla [**55**].

CONJECTURE 1. *If $f, f_1, \cdots, f_n \in \mathbb{C}(x)$ satisfy $f = f_1 \circ f_2 \circ \cdots f_n$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$.*

We show that this conjecture does not hold and construct several explicit counterexamples to the conjecture. These can be found in Chapter 2. In light of aforementioned results, that was expected since if $f \in \mathbb{C}(x)$ is arbitrary, then no transitive Dedekind subgroup of $\mathrm{Mon}(f)$ needs to exist.

We further explain the consequences of our general results for two well-studied classes of polynomials, namely additive polynomials and subadditive polynomials. Additive polynomials over a field K are those that satisfy the identity $f(x+y) = f(x) + f(y)$. It is well known and easy to see that if K is a field of characteristic $p > 0$, then additive polynomial over K are exactly the polynomials of the form $f(x) = a_n x^{p^n} + a_{n-1}x^{p^{n-1}} + \cdots + a_1 x^p + a_0 x$, and if $\mathrm{char}(K) = 0$, the only additive polynomials over K are $f(x) = a_0 x$ for some $a_0 \in K$; see [**66**, Ch. 3] for a proof and more details on additive polynomials. Note that if $\mathrm{char}(K) > 0$ and f is additive over K, then $\mathrm{char}(K) \mid \deg f$ (this is the case to which Ritt's method does not apply). We show that the monodromy group of a separable additive polynomial over a field K of positive characteristic has a transitive abelian subgroup, so that our general results can be applied to additive polynomials. Note that an additive polynomial $f(x)$ is separable exactly when $f'(x) \neq 0$. We prove the following theorem.

THEOREM 3. *Let K be a field of characteristic $p > 0$ and let $f(x) \in K[x]$ be a separable additive polynomial.*

i) Any complete decomposition of $f(x)$ can be obtained from any other complete decomposition of $f(x)$ through finitely many steps, where in each step we replace a complete decomposition of $f(x)$ by a Ritt neighbor.

ii) If $f_1 \circ f_2 \circ \cdots \circ f_m = f = g_1 \circ g_2 \circ \ldots \circ g_n$ are two complete decompositions of $f(x)$ in $K[x]$, then $m = n$ and there is a permutation π of $\{1, 2, \ldots, m\}$ such that $\mathrm{Mon}(f_i) \cong \mathrm{Mon}(g_{\pi(i)})$ for each i. It follows that $\deg f_i = \deg g_{\pi(i)}$ and $\gamma(f_i) = \gamma(g_{\pi(i)})$.

iii) If $f_1, f_2, \ldots, f_m \in K[x]$ satisfy $f = f_1 \circ f_2 \circ \cdots \circ f_m$, then

$$\gamma(f) \mid \gamma(f_1)\gamma(f_2)\ldots\gamma(f_m).$$

Additive polynomials have been widely studied ever since Ore's papers [**73, 74**] in 1933. In [**74**] Ore proved that any two complete decompositions of a separable additive polynomial consist of the same number of indecomposables and moreover that the sequences of degrees of indecomposables are the same up to permutation. We note that Ore's proof is completely different from ours. In particular, while both proofs show that any complete decomposition of an additive polynomial can be obtained from any other such decomposition through finitely many steps, our steps involve replacing two adjacent indecomposables by two others having ths same composition, whereas Ore's steps replace a block of $m \geq 2$ consecutive indecomposables by another block of m indecomposables which have the same composition, where the degrees of the second batch of indecomposables are a circular shift of the degrees of the first batch of indecomposables. Moreover, since Ore does not use Galois closures or monodromy groups, his methods do not give information about the other parts of Theorem 3.

We further prove that the analogous results hold for subadditive polynomials. If K is a field of characteristic $p > 0$, a polynomial $S \in K[x]$ is said to be subadditive if there exists a separable additive $f \in K[x]$ and $n \in \mathbb{N}$ coprime to p such that $S(x^n) = f(x)^n$. There is a series of papers on subadditive polynomials [**20, 21, 56, 57**], in which several interesting properties of these polynomials are exposed, including partial results on decomposition properties of subadditive polynomials. These results rely on Ore's arguments and long computations involving factors of $S(x^n) - S(y^n)$. In proving our stronger results we recover most of these results and we give new and much shorter proofs.

We remark that additive and subadditive polynomials are well-studied classes of polynomials also in the following context. It is well known that if $\mathrm{char}(K) \nmid \deg f$ and $f(x)$ is indecomposable over K, then $f(x)$ is also indecomposable over any extension field of K, see for instance [**89**, Ch. 1, Thm. 6]. The extent of failure of this statement in the case when $\mathrm{char}(K) \mid \deg f$ is a well-investigated topic. Dorey and Whaples [**25**] were first to point out that if $\mathrm{char}(K) \mid \deg f$, there exist indecomposable $f \in K[x]$ which are decomposable over some extension field of K. A method for finding such counterexamples had already been supplied by Ore [**74**] in 1933, who showed that an indecomposable additive polynomial $f \in K[x]$, where $\mathrm{char}(K) = p > 0$, can be represented as a functional composition of additive polynomials over $\overline{K}$ of degree p. Until 1993, when [**44**] appeared, the only known counterexamples involved additive and subadditive polynomials. Further families of counterexamples as well as description of all such polynomials can be found in [**52, 53, 70, 64**].

2. Diophantine equations

Ritt's polynomial decomposition results have been applied to a variety of topics. As already mentioned, one such topic is the classification of polynomials $f, g \in \mathbb{Q}[x]$ such that the equation $f(x) = g(y)$ has infinitely many integer solutions. In 2000, Bilu and Tichy [**13**] presented a complete and definite answer to this problem. In what follows we recall the result of Bilu and Tichy and explain the historical background of the problem.

We say that the equation $f(x) = g(y)$ has infinitely many *rational solutions with a bounded denominator* if there exists $\lambda \in \mathbb{N}$ such that $f(x) = g(y)$ has infinitely many solutions $x, y \in \mathbb{Q}$ that satisfy $\lambda x, \lambda y \in \mathbb{Z}$. If the equation $f(x) = g(y)$ has only finitely many rational solutions with a bounded denominator, then it clearly has only finitely many integer solutions.

We further need to define five kinds of so-called *standard pairs* of polynomials. In what follows a and b are nonzero rational numbers, m and n are positive integers, $r \geq 0$ is an integer, $p(x) \in \mathbb{Q}[x]$ is a nonzero polynomial (which may be constant) and $D_m(x, a)$ is the m-th Dickson polynomial with parameter a, defined by the functional equation

$$D_m\left(x + \frac{a}{x}, a\right) = x^m + \left(\frac{a}{x}\right)^m.$$

Standard pairs of polynomials over $\mathbb{Q}$ are listed in the following table.

kind	standard pair (or switched)	parameter restrictions
$first$	$(x^m, ax^r p(x)^m)$	$r < m, (r, m) = 1,\ r + \deg p > 0$
$second$	$(x^2, (ax^2 + b)p(x)^2)$	-
$third$	$(D_m(x, a^n), D_n(x, a^m))$	$(m, n) = 1$
$fourth$	$(a^{\frac{-m}{2}} D_m(x, a), -b^{\frac{-n}{2}} D_n(x, b))$	$(m, n) = 2$
$fifth$	$((ax^2 - 1)^3, 3x^4 - 4x^3)$	-

THEOREM 4 (Bilu and Tichy, 2000). *Let $f(x)$ and $g(x)$ be non-constant polynomials in $\mathbb{Q}[x]$. Then the following assertions are equivalent.*

- *The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator;*
- *We have*

$$f(x) = \varphi\left(f_1\left(\lambda(x)\right)\right), \quad g(x) = \varphi\left(g_1\left(\mu(x)\right)\right),$$

where $\varphi(x) \in \mathbb{Q}[x]$, $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ are linear polynomials, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.

The proof of Theorem 4 relies on Siegel's classical theorem [**90**] on integral points on curves, and is consequently ineffective. Davenport, Lewis and

Schinzel [**22**] were first to obtain a finiteness criterion for the equation $f(x) = g(y)$, but it was far from explicit and well-applicable. Fried [**43**] presented a quite general finiteness criterion, but still very restrictive for applications. Siegel's theorem implies that the finiteness problem for the equation $f(x) = g(y)$ reduces to the question of whether or not the corresponding plain curve has a component of genus 0 and with at most 2 points at infinity. Fried [**43**] further showed that this question reduces to two independent problems, one of which is when a polynomial of the form $f(x) - (y)$ has a quadratic factor and the other is a special version of Ritt's second theorem. First problem was resolved by Bilu [**11**]. Schinzel [**88**] obtained a completely explicit finiteness criterion for the equation $f(x) = g(y)$ under the assumption $(\deg f, \deg g) = 1$. Bilu and Tichy [**13**] followed the approach of Fried [**43**] and Schinzel [**88**], but also employed several new ideas to avoid Schinzel's assumption $(\deg f, \deg g) = 1$, and so proved Theorem 4.

Theorem 4 proved to be suitable for applications; the applications include Diophantine equations with power-sum polynomials [**12, 62, 80**], orthogonal polynomials [**92**], polynomials arising from counting combinatorial objects [**14, 77, 92**], and several other families of polynomials [**34, 61, 76**].

Methods and results. Proving that the equation of the type $f(x) = g(x)$ has only finitely many integer solutions by using Bilu–Tichy theorem, reduces to showing that polynomials $f(x)$ and $g(x)$ can not be written as $f(x) = \varphi(f_1(\lambda(x)))$ and $g(x) = \varphi(g_1(\mu(x)))$, in notation of Theorem 4. The first and the key step in applications is to determine possible decompositions of $f(x)$ and $g(x)$. This step usually requires applying some general results on polynomial decomposition, such as those of Ritt [**84**] and Schinzel [**89**, Ch. 1] that were mentioned earlier in this introduction, but the success in completing this step depends on particular properties of polynomials $f(x)$ and $g(x)$ and is by no means guaranteed. Sufficient conditions for f to be indecomposable or to have decompositions only of certain type, were systematically treated in [**31, 32, 92**]. If one succeeds in finding possible decompositions of $f(x)$ and $g(x)$ (or at least enough information about them), further steps in applications of Theorem 4 to the equation $f(x) = g(y)$ are usually technical and lengthy, but possible to complete; they consist of comparing possible decompositions of $f(x)$ and $g(x)$ with those prescribed in Theorem 4.

In Chapter 3 we prove the finiteness theorems for two concrete Diophantine equations using Theorem 4. We show that the equation $-1^k+2^k-\cdots+(-1)^x x^k = g(y)$, with $g \in \mathbb{Q}[x]$, has only finitely many integer solutions unless $g(x)$ can be decomposed in ways that we list explicitly. It is well known that the alternating power sum $-1^k+2^k-\cdots+(-1)^x x^k$ is closely related to the k-th Euler polynomial, see Chapter 3 for more details. As a side result, we give a complete description

of possible decompositions of Euler polynomials into polynomials with complex coefficients. Since Euler polynomials appear in many classical results and play an important role in various approximation and expansion formulas in discrete mathematics and in number theory (see for instance [**1**], [**15**]), we believe that this result might be of broader interest.

In Chapter 4, we study Diophantine equations involving power sums of arithmetic progressions. For integers a and b with $\gcd(a,b)=1$ and $k,n\in\mathbb{N}$, with $n\geq 2$, we let $S_{a,b}^{k}(n)=b^{k}+(a+b)^{k}+\cdots+(a(n-1)+b)^{k}$. We prove that the equation $S_{a,b}^{k}(x)=S_{c,d}^{l}(y)$ for $2\leq k<l$ has only finitely many solutions in integers x and y. As a special case, that is when $a=c=1, b=d=0$, we obtain the main result of [**12**].

3. Diophantine m-tuples

In this section we give introduction to Chapter 5 that concerns the topic known as Diophantine m-tuples. Greek mathematician Diophantus of Alexandria first studied the problem of finding four numbers such that the product of any two of them increased by 1 is a perfect square. Such set of size m is said to be a *Diophantine m-tuple*. Diophantus found a set of four rationals with the given property, namely the set $\{1/16, 33/16, 17/4, 105/16\}$. Fermat found a first Diophantine quadruple in integers - the set $\{1,3,8,120\}$. The folklore conjecture is that there are no Diophantine quintuples in integers. In 1969, Baker and Davenport [**3**] proved that the set $\{1,3,8\}$ can not be extended to a Diophantine quintuple, which was the first result supporting the conjecture. Moreover, they showed a stronger result by proving that the triple $\{1,3,8\}$ can be extended to a Diophantine quadruple in integers only by adding 120 to the set. An integer N which can replace 120 while preserving the property must satisfy $N+1=x^2$, i.e. must be of the form $N=x^2-1$ and the other two conditions $3N+1=y^2$ and $8N+1=z^2$ correspond to solutions of the following system of Pellian equations

$$3x^2-2=y^2,\quad 8x^2-7=z^2.$$

Thus the question is whether this system of equations has any solutions in positive integers, other than the solutions with $x=1$ and $x=11$, corresponding to $N=0$ and $N=120$, respectively. The solutions to each of these Pellian equations lie in finitely many binary recurrent sequences, so the problem reduces to finding the intersections of these sequences. The proof of Baker and Davenport relies on Baker's theory on linear forms in logarithms of algebraic numbers and a reduction method based on continued fractions. This paper provided a method and consequently opened the door for investigating Diophantine m-tuples.

In 1997, by employing several new ideas and results from Diophantine approximations, such as a result of Rickert [**83**] on simultaneous rational approximations of algebraic numbers, Dujella [**26**] generalized the result of Baker and Davenport by proving that no Diophantine triple of the form $\{k-1, k+1, 4k\}$, with $k \geq 2$, can be extended to a Diophantine quintuple in integers. In 1998, Dujella and Pethő [**33**] showed that not even the pair $\{1, 3\}$ can be extended to a Diophantine quintuple in integers. In 2008, Fujita [**46**] proved that no Diophantine pair $\{k-1, k+1\}$, with $k \geq 2$, can be extended to a Diophantine quintuple in integers. In 2004, Dujella [**29**] showed that there are no Diophantine sextuples in integers and that there are at most 10^{1930} Diophantine quintuples, which was a giant step towards proving the conjecture. This bound was subsequently significantly improved in [**47**] and [**37**], and very recently in [**35**]. It is proved there that there exist at most $6.8 \cdot 10^{32}$ Diophantine quintuples. In light of these results, we may say that the problem of the existence of Diophantine quintuples in integers is almost completely solved.

One way to generalize the problem was to study sets $\{a_1, a_2, \ldots, a_m\}$ of nonzero elements of an arbitrary ring R satisfying $a_i a_j + a$ is a square in R for all $1 \leq i < j \leq m$ and for some $a \in R$. Such sets are said to have property $D(a)$ and they have been studied at least since 1985, see [**17, 51, 69**]. One may further generalize the problem by studying sets $\{a_1, a_2, \ldots, a_m\}$ of nonzero elements in a ring R that satisfy $a_i a_j + a$ is an n-th power in R for all $1 \leq i < j \leq m$ and for some fixed $a \in R$ and $n \geq 2$. These were first studied by Bugeuad and Dujella [**18**]. In 1997, Dujella [**26**] studied sets of Gaussian integers with the property $D(a)$ with $a \in \mathbb{Z}[i]$. Dujela examined the question of the existence of such sets with four or more elements. This was the first paper concerning the size of Diophantine m-tuples in $\mathbb{Z}\left[\sqrt{d}\right]$ with $d \in \mathbb{Z}$. In [**38**] it was shown that no Diophantine triple of the form $\{k-1, k+1, 4k\}$, with $k \in \mathbb{Z}[i]$ and $k \notin \{0, \pm 1\}$, can be extended to a Diophantine quintuple in Gaussian integers. We can extend the triple $\{1, 3, 8\}$ to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{d}\right]$ for some values of d; for instance $\{1, 3, 8, 120, 1678\}$ is a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{201361}\right]$. It is natural to start investigating the upper bound for the size of Diophantine m-tuples in $\mathbb{Z}[\sqrt{d}]$ by focusing on a problem of extensibility of Diophantine triples $\{k-1, k+1, 4k\}$ and Diophantine pair $\{1, 3\}$ to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{d}\right]$, since the problem in integers was approached similarly, see [**27, 33, 46**]. Franušić [**39**] proved that the pair $\{1, 3\}$ can not be extended to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{d}\right]$ if d is a negative integer and $d \neq -2$.

We resolve the case $d = -2$. If $d = -2$ and $\{1, 3, c\}$ is a Diophantine triple in $\mathbb{Z}\left[\sqrt{-2}\right]$, then $c \in \{c_k, d_l\}$, where the sequences (c_k) and (d_l) are defined as

follows

$$c_0 = 0, \qquad c_1 = 8, \qquad c_{k+2} = 14c_{k+1} - c_k + 6;$$
$$d_0 = -1, \qquad d_1 = -3, \qquad d_{l+2} = 14d_{l+1} - d_l + 8.$$

The set $\{1, 3, c_k, d_l\}$ is not a Diophantine quadruple for $k \geq 1$ and $l \geq 0$ since $1 + c_k d_l$ is a negative odd number and hence it can not be a square in $\mathbb{Z}\left[\sqrt{-2}\right]$. Therefore, if there is an extension of the Diophantine pair $\{1, 3\}$ to a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$, then it is of the form $\{1, 3, c_k, c_l\}$, with $l > k \geq 1$ or $\{1, 3, d_k, d_l\}$, with $l > k \geq 0$. We eliminate the possibility of the extension of the set $\{1, 3, c_k, c_l\}$ to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{-2}\right]$ by using the result of Dujella and Pethő [**33**]. The remaining case is much more difficult to handle. We prove the following theorem.

THEOREM 5. *Let k be a nonnegative integer and d an integer. If the set $\{1, 3, d_k, d\}$ is a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$, then $d = d_{k-1}$ or $d = d_{k+1}$.*

We remark that if d is a negative integer and $d \neq -2$, and if $\{1, 3, c\}$ is a Diophantine triple in $\mathbb{Z}\left[\sqrt{d}\right]$, then the case $c = d_k$ can not occur, see [**39**].

In the proof of Theorem 5, we follow a method of Dujella and Pethő [**33**]. Instead of applying linear forms in logarithms, we further use a result of Bennett [**9**] on simultaneous rational approximations of algebraic numbers, that proved suitable for applications in some previous papers on Diophantine m-tuples, such as [**29**]. Theorem 5 implies that the pair $\{1, 3\}$ can not be extended to a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$. Hence, the pair $\{1, 3\}$ can not be extended to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{d}\right]$, where d is a negative integer. As already suggested, this can be considered as a step forward to finding an upper bound for the size of Diophantine m-tuples in $\mathbb{Z}\left[\sqrt{d}\right]$ with $d \in \mathbb{Z}$.

Chapter 2

Invariants of functional decomposition of rational functions

This chapter contains a preliminary version of the paper [**60**] with the title *Invariants of functional decomposition of rational functions*, which is a joint paper with Michael Zieve. This paper is in preparation and is soon going to be submitted for publication.

Abstract. For any rational function $f(X)$ with coefficients in a field K, we examine the structure of an expression of $f(X)$ as the composition $f_1 \circ f_2 \circ \cdots \circ f_m$ where each f_i is an element of $K(X)$ of degree at least two which cannot be written as the composition of lower-degree functions in $K(X)$. Under certain hypotheses, we exhibit several invariants of any such decomposition. This provides a common generalization of results of Ore and Ritt, among others. As special cases, we obtain new proofs of results of Beardon–Ng and Gutierrez–Sevilla; our method also yields several counterexamples to a conjecture of Gutierrez–Sevilla. Finally, we explain the consequences of our general results for two much-studied classes of polynomials, namely additive and subadditive polynomials; in so doing, we recover most of the known results about decompositions of these polynomials, as well as several new results.

1. Introduction

In 1920's, Ritt [**84**] studied functional equations of the type $f_1 \circ f_2 \circ \cdots \circ f_m = g_1 \circ g_2 \circ \cdots \circ g_n$ in non-constant complex polynomials. This led him to study possible ways of writing a complex polynomial as a functional composition of polynomials of lower degree. A polynomial $f \in \mathbb{C}[X]$ with $\deg f > 1$ is called *indecomposable* if it cannot be written as the composition $f(X) = g(h(X))$ with

$g, h \in \mathbb{C}[X]$ and $\deg g, \deg h > 1$. By induction it follows that any polynomial $f(X)$ with $\deg f > 1$ can be written as a composition of indecomposable polynomials – such an expression of $f(X)$ is said to be a *complete decomposition* of $f(X)$. Ritt proved that one can obtain any complete decomposition of $f(X)$ from any other through finitely many steps, where each step consists of replacing two adjacent indecomposable polynomials by two others with the same composition. This result is known in literature as Ritt's first theorem.

Ritt then solved the equation $a \circ b = c \circ d$ in indecomposable $a, b, c, d \in \mathbb{C}[X]$. In so doing, Ritt noticed that in every solution of the equation, the degrees of $a(X)$ and $b(X)$ are the same as those of $c(X)$ and $d(X)$, though possibly in a different order. From Ritt's first theorem it follows that the number of indecomposable polynomials in any two complete decomposition of $f(X)$ is the same, as well as the sequences of degrees of indecomposable polynomials (up to permutation). In 2000, Beardon and Ng [**8**] presented another invariant of polynomial decomposition. Writing $\Gamma(f)$ for the set of linear $\ell \in \mathbb{C}[X]$ such that $f \circ \ell = f$, and $\gamma(f)$ for the size of $\Gamma(f)$, Beardon and Ng showed that if $f = f_1 \circ f_2 \circ \cdots \circ f_n$ is a complete decomposition of $f \in \mathbb{C}[X]$, then the sequence $(\gamma(f_1), \gamma(f_2), \ldots, \gamma(f_n))$ is uniquely determined (up to permutation) by $f(X)$. They further showed that if $f, f_1, \ldots, f_n \in \mathbb{C}[X]$ satisfy $f = f_1 \circ f_2 \circ \cdots f_n$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$. Very recently, Zieve and Müller [**96**] presented a new invariant which generalizes both Ritt's degree invariant and the invariant of Beardon and Ng. They showed that if $f = f_1 \circ f_2 \circ \cdots \circ f_n$ is a complete decomposition of $f \in \mathbb{C}[X]$, then the sequence of monodromy groups $(\mathrm{Mon}(f_1), \mathrm{Mon}(f_2), \ldots, \mathrm{Mon}(f_n))$ is uniquely determined (up to permutation) by $f(X)$, where the monodromy group $\mathrm{Mon}(f_i)$ denotes, as usual, the Galois group of the Galois closure of $\mathbb{C}(x)/\mathbb{C}(f_i(x))$, viewed as a permutation group on the conjugates of x over $\mathbb{C}(f_i(x))$.

These results hold over fields other than the complex numbers. Engstrom [**36**] and Levi [**65**] proved the analogues of Ritt's results in the case of fields of characteristic zero, Fried and McRae [**45**] proved them in the case of fields of positive characteristic when the degree of the polynomial under consideration is not divisible by the characteristic of the underlying field. It is explained in [**96**] that the monodromy invariant holds also for polynomials that satisfy the latter condition. Gutierrez and Sevilla [**55**] showed that in this case also $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$ when $f = f_1 \circ f_2 \circ \cdots f_n$.

In this paper, we examine the analogues of the aforementioned results for rational functions with coefficients in an arbitrary field, and prove that these invariants remain valid under certain hypothesis on the monodromy group. We follow a Galois-theoretic method for addressing decomposition questions, that

was developed by Ritt [**84**] and simplified and modernized in [**96**]. The approach we take clarifies the reason why these results are true in some settings and not in others. The importance of the monodromy group when studying various questions about polynomials, in particular decomposition questions, was exhibited by Fried in [**41, 42, 45**].

Ritt [**84**] noticed that if $f \in \mathbb{C}[X]$, then the inertia group I at any infinite place of (the Galois closure of) $\mathbb{C}(x)/\mathbb{C}(f(x))$ is a transitive cyclic subgroup of $\mathrm{Mon}(f)$. The same holds if $f \in K[X]$, where K is a field such that $\mathrm{char}(K) \nmid \deg f$. In that case, one can translate questions about decompositions of $f(X)$ into questions about subgroups of I, which are possible to resolve since I is cyclic, see [**96**] for details. A transitive cyclic subgroup of $\mathrm{Mon}(f)$ does not need to exist when $f \in K[X]$ with $\mathrm{char}(K) \mid \deg f$, nor when $f \in K(X)$ is arbitrary. Dorey and Whaples [**25**] were first to provide an example of a polynomial $f(X)$ with coefficients in a field K with $\mathrm{char}(K) \mid \deg f$, that has two complete decompositions consisting of a different number of indecomposables. Ritt himself [**85, 86**] studied decomposition questions for complex rational functions and had noticed that a certain rational function of degree 12 can be represented as a composition of two and as a composition of three indecomposable complex rational functions. This and further families of counterexamples to the rational functions analogues of Ritt's results can be found in [**67**]. It is further noted there that all known counterexamples to the rational function analogues of Ritt's results fall into certain classes, which suggests that there might be a precise description of all such counterexamples, but that present techniques seem to be insufficient for proving such results. Very few results on rational function decomposition exist. Among best ones is still Ritt's result on commuting rational functions [**85**]. See also [**95**] where the analogues of Ritt's results are shown for Laurent polynomials.

In this paper, we examine decompositions properties of rational functions whose monodromy group has a transitive quasi-Hamiltonian subgroup, and then of those whose monodromy group has a transitive Dedekind subgroup. A group A is said to be *quasi-Hamiltonian* if the product of any two subgroups of A is a group. Note that the product of two subgroups I, J of A is a group if and only if $IJ = JI$. A group is said to be Dedekind it it has no nonnormal subgroups. Note that all abelian groups are Dedekind groups and all Dedekind groups are quasi-Hamiltonian. A non-abelian Dedekind group is called a Hamiltonian group. Dedekind [**23**] showed that finite Hamiltonian groups consist of the direct products of the order-8 quaternion group with an abelian group containing no elements of order 4. Iwasawa [**58**] showed a similar structural result for quasi-Hamiltonian groups.

In Section 3 we prove that if $f(X)$ has coefficients in an arbitrary field, $f'(X) \neq 0$, and the monodromy group of $f(X)$ has a transitive quasi-Hamiltonian subgroup, then an analogue of Ritt's first theorem holds for $f(X)$, i.e. any complete decomposition of f can be obtained by any other by repeatedly replacing two adjacent indecomposable rational functions by two others with the same composition. In Section 4, we prove that if $f'(X) \neq 0$ and if the monodromy group of $f(X)$ has a transitive Dedekind subgroup, then the pairs of indecomposables (a, b) and (c, d) such that $f = a \circ b = c \circ d$ have the same pair of monodromy groups, possibly in reversed order. Under the same hypothesis on $f(X)$, in Section 5 we prove that if rational functions $f, f_1, \ldots, f_n$ with coefficients in a field K satisfy $f = f_1 \circ f_2 \circ \cdots \circ f_n$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$, where $\gamma(f) = |\{\mu \in K(X) : f(\mu(X)) = f(X)\}|$. In this way we generalize and give new proofs of the aforementioned results of Beardon–Ng [**8**]. In [**55**] Gutierrez and Sevilla conjectured that if $f, f_1, \cdots, f_n \in \mathbb{C}(X)$ satisfy $f = f_1 \circ f_2 \circ \cdots f_n$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$. In Section 5 we show that this conjecture does not hold. In light of aforementioned results, that was expected since if $f \in \mathbb{C}(X)$ is arbitrary, then no transitive Dedekind subgroup of $\mathrm{Mon}(f)$ needs to exist. Several explicit counterexamples to the conjecture can be found in Section 5.

In the last two sections, we discuss consequences of our general results for two widely-studied classes of polynomials, namely additive and sub-additive polynomials. The Definitions of additive and subadditive polynomials will be given in Section 6 and Section 7, respectively. We prove the analogues of the aforementioned results by Ritt, Beardon–Ng, Gutierrez-Sevilla, Zieve-Müller for both additive and subadditive polynomials. In proving these results, we recover most of the known results on decompositions of additive and subadditive polynomials, such as those in [**19, 21, 25, 57, 73, 74**].

2. Notation and preliminary results

In this section we present some preliminary results which will be used in the paper.

Let K be a field and $f \in K(X)$. We define a *decomposition* of $f(X)$ to be an expression $f = f_1 \circ \cdots \circ f_n$ with $f_i \in K(X)$ and $\deg f_i > 1$. We say that $f(X)$ with $\deg f > 1$ is *indecomposable* if it has no decomposition of length $n > 1$. A *complete decomposition* of $f(X)$ is an expression of $f(X)$ as the composition of indecomposable rational functions. In what follows, we reduce reduce the study of decompositions of $f(X)$ to the study of subgroups of the monodromy group of $f(X)$, which is defined as follows.

Definition 2.1. Let K be a field. Given a $f \in K(X) \setminus K$ the *monodromy group* $\mathrm{Mon}(f)$ is the Galois group of (the numerator) of $f(X) - t$ over $K(t)$,

where t is transcendental over K, viewed as a group of permutations of the roots of $f(X) - t$.

Write $f(X) = a(X)/b(X)$ where $a(X)$ and $b(X)$ are coprime polynomials in $K[X]$. Let t be transcendental over K and let L be the splitting field of $\phi(X) := a(X) - t \cdot b(X)$ over $K(t)$. Let x be a root of $f(X) - t$ in L, so that $t = f(x)$. Then $\mathrm{Mon}(f) = \mathrm{Gal}(L/K(f(x))$. Note that $\phi(X)$ is an irreducible polynomial in $K(t)[X]$ (it follows from Gauss's Lemma). If $f'(X) \neq 0$, then $\phi'(X) \neq 0$ as well and $\phi(X)$ is hence separable; then L is the Galois closure of $K(x)/K(f(x))$. Since $\phi(X)$ is irreducible, the monodromy group of $f(X)$, viewed as a group of permutation of the roots of $\phi(X)$, is a transitive group. If Stab_x denotes the stabilizer of x in $\mathrm{Mon}(f)$, then $W \mapsto K(x)^W$ is a bijection from the set of groups between Stab_x and $\mathrm{Mon}(f)$ to the set of fields between $K(x)$ and $K(f(x))$. Lüroth's theorem provides a dictionary between decompositions of $f(x)$ and the increasing chain of fields between $K(f(x))$ and $K(x)$. Indeed, if $f = g \circ h$, with $g, h \in K(X)$, then $K(h(x))$ clearly lies between $K(f(x))$ and $K(x)$. For a non-constant $f(X) \in K(X)$, Lüroth's theorem implies that any field L such that $K(f(x)) \subseteq L \subseteq K(x)$, must be of the form $L = K(h(x))$ for some $h(X) \in K(X)$. Since $f(x) \in K(h(x))$ it follows that $f = g \circ h$ for some $g(X) \in K(X)$. A generator of an intermediate field of $K(x)/K(f(x))$ is not uniquely determined, but it is easy to see that for non-constant $h_1(X), h_2(X) \in K(X)$, we have that $K(h_1(x)) = K(h_2(x))$ if and only if $h_1 = \mu \circ h_2$ for some degree-one $\mu(X) \in K(X)$, which motivates the following definition.

Definition 2.2. For $f \in K(X)$, we say two decompositions $f = f_1 \circ \cdots \circ f_n$ and $f = g_1 \circ \cdots \circ g_m$ of $f(X)$ are *equivalent* if $n = m$ and there are degree-one $\mu_0, \ldots, \mu_n \in K(X)$, with $\mu_0 = \mu_n = X$, such that $g_i = \mu_{i-1} \circ f_i \circ \mu_i^{\langle -1 \rangle}$ for $1 \leq i \leq n$, where $\mu^{\langle -1 \rangle}(X)$ denotes the inverse of $\mu(X)$ with respect to functional composition.

Therefore, the class of decompositions of $f(x)$ that are equivalent to the decomposition $f = f_1 \circ \cdots \circ f_n$ corresponds to the maximal decreasing chain of fields $K(x) \supset K(f_n(x)) \supset K(f_{n-1} \circ f_n(x)) \supset \cdots \supset K(f_1 \circ \cdots \circ f_n(x)) = K(f(x))$, which in turn corresponds to the maximal decreasing chain of groups between $\mathrm{Mon}(f)$ and the point stabilizer in $\mathrm{Mon}(f)$.

Hence, the study of decompositions of $f(X)$ reduces to the study of groups between $\mathrm{Mon}(f)$ and the point stabilizer Stab_x in $\mathrm{Mon}(f)$. If we assume that there exists a transitive quasi-Hamiltonian subgroup A of $\mathrm{Mon}(f)$, then clearly $\mathrm{Mon}(f) = A\mathrm{Stab}_x$; then the study of groups between Stab_x and $\mathrm{Mon}(f)$ reduces to the study of subgroups of A via the following simple lemma.

Lemma 2.3. *Let G be a finite group and A and H subgroups of G such that $G = HA$ and that A is quasi-Hamiltonian. If W is any group lying between*

H and G, then $W = HJ$ where $J = W \cap A$ and $H \cap J = H \cap A$. If W_1 and W_2 are groups between H and G and if we denote $J_i := W_i \cap A$, $i = 1, 2$, then $W_1 \cap W_2 = H(J_1 \cap J_2)$ and $\langle W_1, W_2 \rangle = HJ_1J_2$.

PROOF. We prove only that $\langle W_1, W_2 \rangle = HJ_1J_2$. The proofs of other claims are similar and simple. Since A is quasi-Hamiltonian, it follows that J_1J_2 is a subgroup of A. Since $HJ_1 = J_1H$ and $HJ_2 = J_2H$, we have that $HJ_1J_2 = J_1HJ_2 = J_1J_2H$, wherefrom it follows that HJ_1J_2 is a group. Clearly $W_1 = HJ_1 \leq HJ_1J_2$ and $W_2 = HJ_2 \leq HJ_1J_2$ and hence $W := \langle W_1, W_2 \rangle \leq HJ_1J_2$. Since $W = HJ$, where $J = W \cap A$, and since $W_1, W_2 \leq W$, it follows that $J_i = W_i \cap A \leq W \cap A = J$ for $i = 1, 2$. Then $J_1J_2 \leq J$, wherefrom $HJ_1J_2 \leq HJ = W$, so $W = HJ_1J_2$. □

3. Ritt's first theorem

In this section we show that if the monodromy group of a rational function $f(X)$ has a transitive quasi-Hamiltonian subgroup, then an analogue of Ritt's first theorem holds for $f(X)$, i.e any two complete decompositions of $f(X)$ can be obtained one from another by repeatedly replacing two adjacent indecomposable rational functions by two others with the same composition.

DEFINITION 3.1. Let K be a field and $f \in K(X)$. We say that two complete decompositions $f = f_1 \circ \cdots \circ f_n$ and $f = g_1 \circ \cdots \circ g_n$ of $f(X)$ are Ritt neighbors if there exists i with $1 \leq i < n$, such that $f_j = g_j$ for all $j \notin \{i, i+1\}$ and $f_i \circ f_{i+1} = g_i \circ g_{i+1}$.

THEOREM 3.2. *Let K be a field and $f \in K(X)$ such that $f'(X) \neq 0$. If the monodromy group of $f(X)$ has a transitive quasi-Hamiltonian subgroup, then any complete decomposition of $f(X)$ can be obtained from any other complete decomposition of $f(X)$ through finitely many steps, where in each step we replace a complete decomposition of $f(X)$ by a Ritt neighbor.*

We prove Theorem 3.2 by translating it into the following group-theoretic statement.

LEMMA 3.3. *Let G be a finite group and A and H subgroups of G such that $G = HA$ and A is quasi-Hamiltonian. Let $H = V_0 < V_1 < \ldots < V_n = G$ and $H = W_0 < W_1 < \ldots < W_m = G$ be two maximal chains of groups. Then one can pass from the first chain to the second chain in finitely many steps, where in each step we replace a chain $H = C_0 < C_1 < \cdots < C_k = G$ by a chain $H = D_0 < D_1 < \cdots < D_k = G$, where $D_i = C_i$ for all i except for one value j between 0 and k.*

PROOF. Suppose that the result does not hold for G, A, H that satisfy the assumptions of the theorem and are such that $|A|$ is minimal among all counterexamples. By Lemma 2.3 it follows that $V_i = HJ_i$, where $J_i = V_i \cap A$, and analogously $W_i = HK_i$ where $K_i = W_i \cap A$, and furthermore that $H \cap J_i = H \cap K_i = H \cap A$. If $V_{n-1} = W_{m-1}$, then we would have a smaller counterexample, since $V_{n-1} = HJ_{n-1}$ and J_{n-1} is also quasi-Hamiltonian, since it is a subgroup of A. Hence $V_{n-1} \neq W_{m-1}$ and consequently $\langle V_{n-1}, W_{m-1} \rangle = G$, since the chains are maximal. Then again by Lemma 2.3 it follows that $\langle V_{n-1}, W_{m-1} \rangle = HJ_{n-1}K_{m-1}$, wherefrom $J_{n-1}K_{m-1} = A$. Let U be a group between $V_{n-1} \cap W_{m-1}$ and V_{n-1}. Then Lemma 2.3 implies that $V_{n-1} \cap W_{m-1} = H(J_{n-1} \cap K_{m-1})$, and $U = HJ$, where $J = U \cap A$, and hence $J_{n-1} \cap K_{m-1} \leq J \leq J_{n-1}$, wherefrom it follows that $J \cap K_{m-1} = J_{n-1} \cap K_{m-1}$. Let $\tilde{U} = \langle U, W_{m-1} \rangle$. Then by Lemma 2.3 it follows that $\tilde{U} = HJK_{m-1}$. Then

$$\begin{aligned}[\tilde{U} : W_{m-1}] &= \frac{|J|}{|J \cap K_{m-1}|} = \frac{|J|}{|J_{n-1} \cap K_{m-1}|} \\ &= [U : (V_{n-1} \cap W_{m-1})].\end{aligned}$$

Analogously

$$[G : \tilde{U}] = \frac{|HJ_{n-1}K_{m-1}|}{|HJK_{m-1}|} = \frac{|J_{n-1}|}{|J|} = [V_{n-1} : U].$$

Therefrom it follows that if U is properly between $V_{n-1} \cap W_{m-1}$ and V_{n-1}, then $\tilde{U}$ is properly between W_{m-1} and G, which can not be, since W_{m-1} is maximal in G. Hence there are no groups properly between $V_{n-1} \cap W_{m-1}$ and V_{n-1}. Let $H = E_0 < E_1 < \ldots < E_k = V_{n-1} \cap W_{m-1}$ be a maximal chain of groups. Then the chain $H = E_0 < E_1 < \ldots < E_k < V_{n-1} < V_n = G$ is also maximal. By the hypothesis we can pass from the chain $H = V_0 < V_1 < \ldots < V_{n-1} < V_n = G$ to the chain $H = E_0 < E_1 < \ldots < E_k < V_{n-1} < V_n = G$ by required steps. In one more step, we can pass from the chain $H = E_0 < E_1 < \ldots < E_k < V_{n-1} < V_n = G$ to the chain $H = E_0 < E_1 < \ldots < E_k < W_{m-1} < W_m = G$. Finally, by the hypothesis, we can pass from the chain $H = E_0 < E_1 < \ldots < E_k < W_{m-1} < W_m = G$ to the chain $H = W_0 < W_1 < \ldots < W_{m-1} < W_m = G$ by required steps □

PROOF OF THEOREM 3.2. Let G be the monodromy group of $f(X)$ and H the point stabilizer in $\mathrm{Mon}(f)$. Then by assumption $G = HA$ for some quasi-Hamiltonian subgroup A of G. Since (the equivalence class of) any complete decomposition of $f(X)$ corresponds to the maximal chain of groups between H and G, Lemma 3.3 completes the proof. □

REMARK 3.4. In [**63**] it is proved that under the same hypothesis on $f(X)$ as in Theorem 3.2, any two complete decompositions of $f(X)$ consist of the same

number of indecomposable polynomials. The proofs there are simple, but note that this result is weaker than the Theorem 3.2. To the proof of Theorem 3.2, Lemma 3.3 was of crucial importance. This lemma is a generalization of the [**96**, Lem. 2.10].

4. The monodromy invariant

Let K be an arbitrary field. Next we study the equation $f = a \circ b = c \circ d$ in indecomposable $a, b, c, d \in K(X)$, under the assumption that $f \in K(X)$ has a nonzero derivative and $\mathrm{Mon}(f)$ has a transitive Dedekind subgroup. We prove that the pairs (a, b) and (c, d) have the same pair of monodromy groups, possibly in reversed order. This generalizes [**96**, Thm. 2.13].

THEOREM 4.1. *Let K be a field and $f \in K(X)$ such that $f'(X) \neq 0$. If the monodromy group of $f(X)$ has a transitive Dedekind subgroup and if $f = a \circ b = c \circ d$, where $a, b, c, d \in K(X)$ are indecomposable, then*

i) either there is a degree-one rational function $\mu \in K(X)$ such that $a = c \circ \mu$ and $b = \mu^{\langle -1 \rangle} \circ d$,

ii) or $\mathrm{Mon}(a)$ *and* $\mathrm{Mon}(d)$ *are isomorphic permutation groups, and so are* $\mathrm{Mon}(b)$ *and* $\mathrm{Mon}(c)$*; in which case* $\deg a = \deg d$ *and* $\deg b = \deg c$.

We first recall the definition of isomorphic permutation groups.

DEFINITION 4.2. Let G and $\tilde{G}$ be permutation groups acting on sets S and $\tilde{S}$, respectively. We say that G and $\tilde{G}$ are isomorphic as permutation groups if there is a group isomorphism $\phi : G \to \tilde{G}$ and a bijection $\psi : S \to \tilde{S}$ such that $\psi(\omega^\tau) = \psi(\omega)^{\phi(\tau)}$ for each $\omega \in S$ and $\tau \in G$.

We prove Theorem 4.1 by translating it into a group-theoretic statement. In what follows, the core of a subgroup W of G denotes, as usual, the intersection of all conjugates of W in G, that is the largest normal subgroup of G contained in W. Consider the action of G on the set G/W of left cosets of W in G by left multiplication; then $\mathrm{core}_G(W)$ is the kernel of this action, so the quotient $G/\mathrm{core}_G(W)$ embeds into the symmetric group $\mathrm{Sym}(G/W)$.

The following lemma is crucial to the proof of Theorem 4.1.

LEMMA 4.3. *Let G be a finite group and A and H subgroups of G such that* $\mathrm{core}_G(H) = 1$, *$G = HA$ and A is Dedekind. Let $H \lneqq W_1 \lneqq G$ and $H \lneqq W_2 \lneqq G$ be two maximal chains of groups such that $W_1 \cap W_2 = H$ and $G = \langle W_1, W_2 \rangle$. Let N be the core of W_1 in G, and let C be the core of H in W_2. Then G/N and W_2/C are isomorphic permutation groups, seen as subgroups of* $\mathrm{Sym}(G/W_1)$ *and* $\mathrm{Sym}(W_2/H)$.

PROOF. Since N is normal in G, it follows that NW_2 is a subgroup of G, $N \cap W_2$ is a normal subgroup of W_2, and $NW_2/N \cong W_2/(N \cap W_2)$. Note that

$$C = \bigcap_{g \in W_2} H^g = \bigcap_{g \in W_2} (W_1 \cap W_2)^g = \left(\bigcap_{g \in W_2} W_1^g \right) \cap W_2$$
$$= \left(\bigcap_{g \in G} W_1^g \right) \cap W_2 = N \cap W_2.$$

Since W_2 is maximal in G and NW_2 contains W_2, it follows that either $NW_2 = G$ or $NW_2 = W_2$. If $G = NW_2$, then it follows that G/N and W_2/C are isomorphic groups. One verifies directly that these are moreover isomorphic permutation groups with respect to their actions on the coset spaces W_2/H and G/W_1, respectively. If on the other hand $NW_2 = W_2$, then $N \leq W_2$. Since $N \leq W_1$ by definition, it follows that $N \leq W_1 \cap W_2 = H$. Since N is a normal subgroup of G and $\mathrm{core}_G(H) = 1$, it follows that $N = 1$, wherefrom $C = N \cap W_2 = 1$. Note that

$$N = \bigcap_{g \in G} W_1^g = \bigcap_{g \in A} W_1^g \geq \bigcap_{g \in A} (W_1 \cap A)^g = \bigcap_{g \in A} J_1^g,$$

Since $N = 1$, it follows that the core of J_1 in A is trivial. But A is Dedekind, so $\mathrm{core}_A(J_1) = J_1$, wherefrom $J_1 = 1$ and $W_1 = HJ_1 = H$, contradiction. □

PROOF OF THEOREM 4.1. Let G denote the monodromy group of $f(X)$ and H the point stabilizer in G. Let x be transcendental over K. Let W_1 and W_2 be subgroups of G fixing $b(x)$ and $d(x)$ respectively, so $H \leq W_1, W_2 \leq G$. Let $W := \langle W_1, W_2 \rangle$. Then the chain of groups $H \leq W_1 \cap W_2 \leq W_1 \leq W \leq G$ corresponds to the chain of fields $K(x) \geq K(h(x)) \geq K(b(x)) \geq K(\hat{a}(b(x)) \geq K(f(x))$, where $h, \hat{a} \in K(x)$. Then clearly $b = \hat{b} \circ h$ for some $\hat{b} \in K(x)$ and $a \circ b = f = g \circ \hat{a} \circ b$, wherefrom $a = g \circ \hat{a}$ for some $g \in K(x)$. Analogously, the chain of groups $H \leq W_1 \cap W_2 \leq W_2 \leq W \leq G$ corresponds to the chain of fields $K(x) \geq K(h(x)) \geq K(d(x)) \geq K(\hat{a}(b(x)) \geq K(f(x))$, so $d = \hat{d} \circ h$ and $\hat{a} \circ b = \hat{c} \circ d$ with $\hat{c}, \hat{d} \in K(x)$, whence $c = g \circ \hat{c}$ and $\hat{a} \circ \hat{b} = \hat{c} \circ \hat{d}$. Since $a, b, c, d \in K(x)$ are indecomposable, if either $\deg g > 1$ or $\deg h > 1$, then there exists a degree-one rational function $\mu \in K(x)$ such that $a = c \circ \mu$ and $b = \mu^{-1} \circ d$. Indeed, if $\deg g > 1$, then $\deg \hat{a} = \deg \hat{c} = 1$ and $\mu = \hat{c}^{\langle -1 \rangle} \circ \hat{a}$. If $\deg h > 1$, then $\deg \hat{b} = \deg \hat{d} = 1$ and $\mu = \hat{d} \circ \hat{b}^{\langle -1 \rangle}$.

It remains to consider the case when $\deg g = 1$ and $\deg h = 1$. If $\deg g = 1$, then $f(x) = \hat{a}(b(x))$ and hence $K(f(x)) = K(\hat{a}(b(x))$, wherefrom $W = G$. If $\deg h = 1$, then $K(h(x)) = K(x)$ and hence $W_1 \cap W_2 = H$. Let N be the core of W_1 in G. The quotient G/N embeds into the symmetric group $\mathrm{Sym}(G/W_1)$ and is isomorphic to $\mathrm{Mon}(a)$. Let C be the core of H in W_2. Then W_2/C embeds

into the symmetric group $\mathrm{Sym}(W_2/H)$ and is isomorphic to $\mathrm{Mon}(d)$. Note that $H \lneqq W_1 \lneqq G$ and $H \lneqq W_2 \lneqq G$ are maximal chains of groups, since a, b, c, d are indecomposable over K. By definition H does not contain a non-trivial normal subgroup of G. By assumption, $G = HA$ for some quasi-Hamiltonian group A. Then from Lemma 4.3 it follows that G/N and W_2/C are isomorphic permutation groups, i.e. $\mathrm{Mon}(a)$ and $\mathrm{Mon}(d)$ are isomorphic permutation groups. By symmetry we have that $\mathrm{Mon}(a)$ and $\mathrm{Mon}(d)$ are isomorphic permutation groups as well. □

Remark 4.4. We do not know whether Theorem 4.1 would remain true if the hypothesis of a transitive Dedekind subgroup were replaced by the weaker hypothesis of a transitive quasi-Hamiltonian subgroup. Any counterexample to this generalization of Theorem 4.1 would have $N = C = 1$ in the notation of Lemma 4.3, but we do not know whether this can happen. The following observations can be easily extracted from the proofs of Theorem 4.1 and Lemma 4.3. If A is quasi-Hamiltonian and such that any nontrivial subgroup of A contains a nontrivial normal subgroup of A, then the case $N = C = 1$ can not occur. If $N = 1$, then $\mathrm{Mon}(a)$ and $\mathrm{Mon}(f)$ are isomorphic groups, but not as permutation groups. What would remain true if the hypothesis of a transitive Dedekind subgroup were replaced by the weaker one of a transitive quasi-Hamiltonian subgroup is that in $f = a \circ b = c \circ d$, either there exists a degree-one rational function $\mu \in K(x)$ such that $a = c \circ \mu$ and $b = \mu^{-1} \circ d$ or $\deg a = \deg d$ and $\deg b = \deg c$. The latter result is proved also in [**63**].

5. The Beardon–Ng invariant

Let K be a field and $f(X) \in K(X)$. Further let $\Gamma(f)$ denote the set of rational functions $\mu \in K(X)$ such that $f \circ \mu = f$ and let $\gamma(f)$ denote the size of the set $\Gamma(f)$. In what follows, we show that if indecomposable $a, b, c, d \in K(X)$ satisfy $f = a \circ b = c \circ d$, where $f \in K(X)$ is such that $f'(X) \neq 0$ and $\mathrm{Mon}(f)$ has a transitive Dedekind subgroup, then $(\gamma(a), \gamma(b)) = (\gamma(c), \gamma(d))$ or $(\gamma(a), \gamma(b)) = (\gamma(d), \gamma(c))$. We further prove that, under the same condition on $f(X)$, if $f = f_1 \circ f_2 \circ \cdots f_n$ for some $f_1, \ldots, f_n \in K(X)$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n)$.

Note that if $f \in K[X]$, then every element of $\Gamma(f)$ is necessarily a polynomial. Beardon and Ng [**8**] showed that both of the aforementioned results hold when $f \in \mathbb{C}[X]$. In [**55**] the latter result is extended to the case when $f, f_1, \ldots, f_n \in K[X]$, where K is a field such that $\mathrm{char}(K) \nmid \deg f$. In this section we give a common generalization of these results. As special cases, we obtain new proofs of these results.

Note that if $f'(X) \neq 0$ and if μ is a degree-one rational function such that $f \circ \mu = f$, then if x is transcendental over K, the maps from $K(x)$ to $K(x)$ which

fix K and map x to $\mu(x)$ are automorphisms of $K(x)$ which fix $K(f(x))$, and vice versa. Hence, $\Gamma(f) \cong \mathrm{Aut}(K(x)/K(f)) \cong N_G(H)/H$, where $G = \mathrm{Mon}(f)$ and H is the point stabilizer in G.

LEMMA 5.1. *Let K be a field and $f(X) \in K(X)$ such that $f'(X) \neq 0$. If $f(X)$ is indecomposable, then*

i) either $\gamma(f) = 1$;
ii) or $f(X)$ is of prime degree, $\mathrm{Mon}(f)$ is cyclic and $\gamma(f) = |\mathrm{Mon}(f)| = \deg f$.

PROOF. Let G be the monodromy group of $f(X)$, H the point stabilizer in G and x transcedental over K. Then $\Gamma(f) \cong N_G(H)/H$. If $f(X)$ is indecomposable, there are no proper groups between H and G, so either $N_G(H) = H$, in which case $\gamma(f) = 1$, or $N_G(H) = G$. In the latter case H is a normal subgroup of G, wherefrom by definition of H and G it follows that $K(x)$ is a normal extension of $K(f(x))$, and hence that $H = 1$. Hence $\gamma(f) = |G| = [K(x) : K(f(x)] = \deg f$. Since there are no proper groups between H and G and $H = 1$, it follows that G is cyclic of prime order. □

COROLLARY 5.2. *Let K be a field and $f(X) \in K(X)$ such that $f'(X) \neq 0$. If the monodromy group of $f(X)$ has a transitive Dedekind subgroup, and $f = a \circ b = c \circ d$ in indecomposable $a, b, c, d \in K(X)$, then*

i) either there is a degree-one rational function $\mu \in K(X)$ such that $a = c \circ \mu$ and $b = \mu^{\langle -1 \rangle} \circ d$; in which case $\gamma(a) = \gamma(c)$ and $\gamma(b) = \gamma(d)$,
ii) or $\gamma(a) = \gamma(d)$ and $\gamma(b) = \gamma(c)$.

PROOF. This is a direct consequence of Theorem 4.1 and Lemma 5.1 □

We further prove the following theorem.

THEOREM 5.3. *Let K be a field and $f(X) \in K(X)$ such that $f'(X) \neq 0$. If the monodromy group of $f(X)$ has a transitive Dedekind subgroup and if $f_1, f_2, \ldots f_m \in K(X)$ satisfy $f = f_1 \circ f_2 \cdots \circ f_n$, then*

$$\gamma(f) \mid \gamma(f_1)\gamma(f_2) \cdots \gamma(f_n).$$

To the proof of Theorem 5.3, we need the following lemma.

LEMMA 5.4. *Let G be a finite group and A and H subgroups of G such that $G = HA$ and A is Dedekind. If W is any group lying between H and G, then*

$$[N_G(H) : H] \mid [N_G(W) : W][N_W(H) : H].$$

PROOF. From Lemma 2.3 it follows that $N_G(H) = HJ$ where $J = N_G(H) \cap A$ and $W = HJ_1$ where $J_1 = W \cap A$ and that $H \cap J = H \cap J_1 = H \cap A$. Then $[N_G(H) : H] = [HJ : H] = |J|/|H \cap J| = |J|/|H \cap A|$. Furthermore, $N_W(H) =$

$W \cap N_G(H) = H(J_1 \cap J)$, again by Lemma 2.3. Hence $[N_W(H) : H] = |J_1 \cap J|/|H \cap A|$. Since $[N_G(W) : W] = |N_G(W)||H \cap A|/|H||J_1|$, it remains to prove that $|N_G(W)|$ is a multiple of $|H||J_1||J|/(|J_1 \cap J||H \cap A|)$. From Lemma 2.3 it follows that $\langle N_G(H), W\rangle = \langle HJ, HJ_1\rangle = HJJ_1$, so

$$\frac{|H||J_1||J|}{|J_1 \cap J||H \cap A|} = |HJJ_1| = |\langle N_G(H), W\rangle|.$$

So, it remains to prove that $|N_G(W)|$ is a mutiple of $|\langle N_G(H), W\rangle|$. To do so it suffices to prove that $N_G(H)$ is a subgroup of $N_G(W)$. Since $J = N_G(H) \cap A$, it follows that J normalizes H. Since A is Dedekind, J normalizes J_1. Then $J \leq N_G(W)$. Since $H \leq W \leq N_G(W)$, it follows that $N_G(H) = HJ \leq N_G(W)$. □

Proof of Theorem 5.3. Let G be the monodromy group of $f(X)$ and H the point stabilizer in G, so that $\Gamma(f) \cong N_G(H)/H$. Let further x be transcedental over K. We first prove that the result holds when $n = 2$. If $f = f_1 \circ f_2$ and W is a subgroup of G fixing $K(f_2(x))$, then $\Gamma(f_1) \cong N_G(W)/W$ and $\Gamma(f_2) \cong N_W(H)/H$. By assumption there exists a Dedekind subgroup A of G such that $G = HA$. From Lemma 5.4 it follows that $\gamma(f) \mid \gamma(f_1)\gamma(f_2)$. Since $H \leq W \leq G$, from Lemma 2.3 we get that $W = HJ$, where $J = W \cap A$. Since A is Dedekind, J is Dedekind as well. Therefore, we may apply Lemma 5.4 to any decomposition of f_2 into two polynomials. Inductively, it follows that if $f = f_1 \circ f_2 \cdots \circ f_n$ for any $n \in \mathbb{N}$, then $\gamma(f) \mid \gamma(f_1)\gamma(f_2)\ldots\gamma(f_n)$. □

The following conjecture was posed by Gutierrez and Sevilla in [**55**].

Conjecture 5.5. *If $f, f_1, \cdots, f_n \in \mathbb{C}(X)$ satisfy $f = f_1 \circ f_2 \circ \cdots f_n$, then*

$$\gamma(f) \mid \gamma(f_1)\gamma(f_2)\cdots\gamma(f_n).$$

In what follows, we show that the Conjecture 5.5 does not hold. In light of Theorem 5.3 that was expected since if $f \in \mathbb{C}(X)$ is arbitrary, then no transitive Dedekind subgroup of the monodromy group of $f(X)$ needs to exist. We first explain a method for finding counterexamples and then construct explicit counterexamples to the Conjecture 5.5.

Let x be transcendental. Since $\Gamma(f) \cong \mathrm{Aut}(\mathbb{C}(x)/\mathbb{C}(f(x)))$, it follows that $\gamma(f) \leq [\mathbb{C}(x) : \mathbb{C}(f(x))] = \deg f$. Note that $\gamma(f) = \deg f$ if and only if the extension $\mathbb{C}(x)/\mathbb{C}(f(x))$ is Galois. In what follows, we explain how to find $f, g, h \in \mathbb{C}(X)$ such that $f = g \circ h$, $\gamma(f) = \deg f$, $\gamma(h) = \deg h$ and $\gamma(g) < \deg g$. Then clearly $\gamma(f) > \gamma(g)\gamma(h)$, which contradicts the conjecture 5.5.

Let G be a finite subgroup of automorphisms of $\mathbb{C}(x)$ that fix $\mathbb{C}$. Then Lüroth's theorem implies that the subfield of $\mathbb{C}(x)$ fixed by G is generated over $\mathbb{C}$ with one rational function; let $f \in \mathbb{C}(X)$ be such that $\mathbb{C}(x)^G = \mathbb{C}(f(x))$. Then $\mathbb{C}(x)/\mathbb{C}(f(x))$ is Galois and $\gamma(f) = \deg f$. Choose $H \leq G$, so that it is not

normal in G. Let $h \in \mathbb{C}(x)$ be such that $\mathbb{C}(x)^H = \mathbb{C}(h(x))$; then $\gamma(h) = \deg h$ and $f(x) = g(h(x))$ for some $g(x) \in \mathbb{C}(x)$, since $\mathbb{C}(f(x)) \subseteq \mathbb{C}(h(x))$. Furthermore, $\Gamma(g) \cong \mathrm{Aut}(\mathbb{C}(x)/\mathbb{C}(g(x))) \cong \mathrm{Aut}(\mathbb{C}(h(x))/\mathbb{C}(f(x)))$. Assume $\gamma(g) = \deg g$. Then

$$|\mathrm{Aut}(\mathbb{C}(h(x))/\mathbb{C}(f(x)))| = \deg g = \deg f/\deg h = [\mathbb{C}(h(x)) : \mathbb{C}(f(x))],$$

which implies that $\mathbb{C}(h(x))$ is a Galois extension of $\mathbb{C}(f(x))$ and H is hence normal in G, a contradiction. Hence, $\gamma(g) < \deg g$.

If G is a finite subgroup of automorphisms of $\mathbb{C}(x)$ which fix $\mathbb{C}$, then Klein showed that G is either cyclic, dihedral, A_4, S_4 or A_5. Therefore, in each case, except when G is cyclic, there exists a subgroup H of G which is not normal in G, and in each such case, we can construct counterexamples. We do that as follows. Starting with any group presentation of the groups D_n, A_4, S_4 or A_5 we find an isomorphic group G of automorphisms of $\mathbb{C}(x)$ that fix $\mathbb{C}$, via generators. We then choose any subgroup H of G, which is not normal in G. Next we need to compute the generator of $\mathbb{C}(x)^G$ and $\mathbb{C}(x)^H$. The main assertion in the proof of Lüroth's theorem is that the generator of the fixed field of G can be found by computing elementary symmetric polynomials in the values $g(x)$ with $g \in G$ until we find one whose value isn't in $\mathbb{C}$; that value $f(x)$ will satisfy $\mathbb{C}(x)^G = \mathbb{C}(f(x))$, see [**54**] for more details. We analogously compute the generator $h(x)$ of $\mathbb{C}(x)^H$. Then there exists a unique $g \in \mathbb{C}(x)$ such that $f = g \circ h$ and we can easily compute it.

Example 5.6. Recall that one group presentation for the symmetric group S_4 is $\langle a, b : a^4 = 1, b^3 = 1, (ab)^2 = 1\rangle$. Let

$$\varphi_1(x) = -\frac{x+1}{x-1} \quad \text{and} \quad \varphi_2(x) = -\frac{x-i}{x+i}.$$

Since $\varphi_1^{(4)}(x) = x$ and $\varphi_2^{(3)}(x) = x$ and $\varphi_3(x) := \varphi_1(\varphi_2(x))$ is such that $\varphi_3^{(2)}(x) = x$, it follows that the group G of automorphisms of $\mathbb{C}(x)$ which fix $\mathbb{C}$, generated with the automorphisms $x \mapsto \varphi_1(x)$ and $x \mapsto \varphi_2(x)$, is isomorphic to S_4. Take H to be a subgroup of G generated with the automorphisms $x \mapsto \varphi_1(x)$ and $x \mapsto \varphi_2(\varphi_1^{(3)}(\varphi_2(x)))$; then $H \cong D_4$ and is hence not normal in G. Then $\mathbb{C}(x)^G = \mathbb{C}(f(x))$ and $\mathbb{C}(x)^H = \mathbb{C}(h(x))$ where

$$f(x) = \frac{x^{24} + 759x^{16} + 2576x^{12} + 759x^8 + 1}{x^4(x^4-1)^4} \quad \text{and} \quad h(x) = \frac{x^8+1}{x^4}.$$

Then $f = g \circ h$ with

$$g(x) = \frac{x^3 + 756x + 2576}{(x-2)^2}.$$

Then by construction $\gamma(f) = \deg f = 24$ and $\gamma(h) = \deg h = 8$. We can easily verify that $\gamma(g) = 1 < \deg g = 3$.

EXAMPLE 5.7. Recall that one group presentation for the alternating group A_4 is $\langle a, b : a^2 = b^3 = (ab)^3 = 1\rangle$. Let

$$\varphi_1(x) = -\frac{1}{x} \quad \text{and} \quad \varphi_2(x) = -\frac{i(x-1)}{x+1}.$$

Then $\varphi_1^{(2)}(x) = x$, $\varphi_2^{(3)}(x) = x$ and $\varphi_3(x) := \varphi_1(\varphi_2(x)))$ is such that $\varphi_3(x)^{(3)}(x) = x$. Then the group G of automorphisms of $\mathbb{C}(x)$ which fix $\mathbb{C}$, generated with the automorphisms $x \mapsto \varphi_1(x)$ and $x \mapsto \varphi_2(x)$, is isomorphic to A_4. Take H to be a subgroup of G generated with $x \mapsto \varphi_1(x)$, so $H \cong C_2$ and H is hence not normal in G. Then $\mathbb{C}(x)^G = \mathbb{C}(f(x))$ and $\mathbb{C}(x)^H = \mathbb{C}(h(x))$ where

$$f(x) = \frac{x^{12} - 33x^8 - 33x^4 + 1}{x^2(x-1)^2(x+1)^2(x^2+1)^2} \quad \text{and} \quad h(x) = \frac{x^2+1}{x}.$$

Then $f = g \circ h$ with

$$g(x) = \frac{(x^2-8)(x^2-2)(x^2+4)}{x^2(x-2)(x+2)}.$$

Then by construction $\gamma(f) = \deg f = 12$ and $\gamma(h) = \deg h = 2$. We can easily verify that $\gamma(g) = 2 < \deg g = 6$.

EXAMPLE 5.8. Recall that one group presentation for the alternating group A_5 is $\langle a, b : a^2 = 1, b^5 = 1, (ab)^3 = 1\rangle$. Let ζ be a primitive 5^{th} root of unity and $\omega = \zeta + 1/\zeta$. Let further

$$\varphi_1(x) = \frac{\omega x + 1}{x - \omega} \quad \text{and} \quad \varphi_2(x) = \zeta^2 x$$

Since $\varphi_1^{(2)}(x) = x$ and $\varphi_2^{(5)}(x) = x$ and $\varphi_3(x) := (\varphi_1(\varphi_2(x)))$ is such that $\varphi_3^{(3)}(x) = x$, it follows that the group G of automorphisms of $\mathbb{C}(x)$ which fix $\mathbb{C}$ generated with the automorphisms $x \mapsto \varphi_1(x)$ and $x \mapsto \varphi_2(x)$, is isomorphic to A_5. Take H to be a subgroup of G generated with the automorphisms $x \mapsto \varphi_2^{(2)}(\varphi_1(\varphi_2(\varphi_1(x)))))$ and $x \mapsto \varphi_1(\varphi_2(x))$; then $H \cong A_4$ and is hence not normal in G. Then $\mathbb{C}(x)^G = \mathbb{C}(f(x))$ and $\mathbb{C}(x)^H = \mathbb{C}(h(x))$ where

$$f(x) = \frac{(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)^3}{x^5(x^{10} + 11x^5 - 1)^5},$$

and

$$h(x) = \frac{x^{12} - 6\zeta^2 x^{10} - 20\zeta^3 x^9 + 15\zeta^4 x^8 - 24x^7 + 24\zeta^2 x^5 + 15\zeta^3 x^4 + 20\zeta^4 x^3 - 6x^2 + \zeta^2}{x(x^{10} + 11x^5 - 1)}.$$

Then $f = g \circ h$ with

$$g(x) = (x + \zeta)^3(x^2 - 3\zeta t + 36\zeta^2).$$

Then by construction $\gamma(f) = \deg f = 60$ and $\gamma(h) = \deg h = 12$. We can easily verify that $\gamma(g) = 1 < \deg g = 5$.

EXAMPLE 5.9. One group presentation for the dihedral group D_n is $\langle a, b : a^2 = 1, b^n = 1, (ab)^2 = 1\rangle$. Let ζ be a primitive n-th root of unity and let

$$\varphi_1(x) = \frac{1}{x} \quad \text{and} \quad \varphi_2(x) = \zeta x$$

Since $\varphi_1^{(2)}(x) = x$, $\varphi_2^{(n)}(x) = x$ and $\varphi_1(\varphi_2(x))^{(2)}(x) = x$, it follows that the group G_n of automorphisms of $\mathbb{C}(x)$ which fix $\mathbb{C}$ generated with the automorphisms $x \mapsto \varphi_1(x)$ and $x \mapsto \varphi_2(x)$ is isomorphic to D_n. Take H_n to be a subgroup of G_n generated with $x \mapsto \varphi_1(x)$; then $H_n \cong C_2$ and H_n is hence not normal in G for $n \geq 3$. Then $\mathbb{C}(x)^{G_n} = \mathbb{C}(f_n(x))$ and $\mathbb{C}(x)^{H_n} = \mathbb{C}(h(x))$ where

$$f_n(x) = x^n + \frac{1}{x^n} \quad \text{and} \quad h(x) = x + \frac{1}{x}.$$

Then $g_n(x) \in \mathbb{C}(x)$ such that $f_n(x) = g_n(h(x))$ is a polynomial of degree n. Then by construction $\gamma(f_n) = \deg f = 2n$, $\gamma(h) = \deg h = 2$ and $\gamma(g_n) < \deg g_n = n$. In particular, if $n = 3$, then

$$f_3(x) = x^3 + \frac{1}{x^3}, \quad h(x) = x + \frac{1}{x}, \quad g_3(x) = x^3 - 3x,$$

and $\gamma(f_3) = \deg f = 6$, $\gamma(h) = \deg h = 2$ and $\gamma(g_3) = 1$.

6. Additive polynomials

In this section we explain the consequences of our general results for additive polynomials. Additive polynomials are defined as follows.

DEFINITION 6.1. If K is a field of characteristic $p \geq 0$, then $f \in K[X]$ is called additive if it satisfies the identity $f(X + Y) = f(X) + f(Y)$.

It is well known that if $\mathrm{char}(K) = p > 0$, the additive polynomials over K are exactly polynomials of the type

$$f(X) = a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \cdots + a_1 X^p + a_0 X,$$

with $a_i \in K$ for $0 \leq i \leq n$, and if $\mathrm{char}(K) = 0$, the only additive polynomials over K are $f(X) = a_0 X$ for some $a_0 \in K$. See [**50**, Chap. 1] for a proof and more details on additive polynomials. Note that an additive polynomial $f(X) \in K[X]$ is separable exactly when $f'(X) \neq 0$.

If K is a field and x is transcendental over K, Soundararajan [**91**] gave necessary and sufficient conditions on $f \in K[X]$ so that $K(x)/K(f(x))$ is Galois. Such polynomials $f(X)$ are closely related to additive polynomials. We now recall the result of Soundararajan.

LEMMA 6.2. *Let K be a field of characteristic $p \geq 0$ and $K(x)$ a simple transcendental extension of K. Let $f(x) \in K[x]$ be of degree $n = p^m \cdot n_1$, $\gcd(p^m, n_1) = 1$. Then $K(x)$ is a Galois extension over $K(f(x))$ if and only if*

(6.2.1) $f(x) = A(g(x))^{n_1} + B$, *where*

$$g(x) = x^{p^m} + a_1 x^{p^{s_1}} + \cdots + a_{r-1} x^{p^{s_{r-1}}} + a_r x + a_{r+1}$$

with n_1 *dividing each* $p^{s_i} - 1$ *and* $a_r \neq 0$, *and* $A, B \in K$.

(6.2.2) K *contains all the roots of* $X^{n_1} = 1$ *and all the roots of* $g(z) = \zeta g(0)$ *for each root* ζ *of* $X^{n_1} = 1$.

For the sake of completeness (since we use Lemma 6.2 in this and in the following section), we explain the main lines of the argument of Soundararajan. One direction is easy. Assume that both (6.2.2) and (6.2.1) hold. Note that then for any $\zeta \in K$ such that $\zeta^{n_1} = 1$ and any $\nu \in K$ such that $g(\nu) = \zeta g(0)$, the automorphisms of $K(x)$ which fix K and map $x \mapsto \zeta x + \nu$, leave $K(f(x))$ fixed. There are clearly $n_1 \cdot \deg g = \deg f$ such automorphisms. Then $\deg f \leq |\mathrm{Gal}(K(x)/K(f(x)))| \leq [K(x) : K(f(x))] = \deg f$, wherefrom it follows that $K(x)/K(f(x))$ is Galois. Proving that the converse also holds is somewhat more difficult. If $K(x)/K(f(x))$ is Galois, then there are exactly $|\mathrm{Gal}(K(x)/K(f(x))| = \deg f$ automorphisms of $K(x)$ that leave $K(f(x))$ fixed. Since $f(x)$ is a polynomial, each of these automorphisms maps $x \mapsto ax + b$ with $a, b \in K$, that satisfy $f(ax + b) = f(x)$. By closer inspection of the equation $f(ax+b) = f(x)$ (that involves multiple comparison of coefficients), Soundararajan proves that there exists a subgroup H of $G = \mathrm{Gal}(K(x)/K(f(x)))$ of size p^m, consisting of the automorphisms of G that map $x \mapsto x + b$ for some $b \in K$. Then he shows that $\tilde{g}(x) = \prod_{\tau \in H} \tau(x)$ is an additive polynomial which is up to constant coefficient the polynomial g from (6.2.1).

Using Lemma 6.2, we can give the following characterization of separable additive polynomials.

LEMMA 6.3. *Let* K *be a field of characteristic* $p > 0$ *and* $f(X) \in K[X]$. *Let* x *be transcendental over* K. *Then the following are equivalent:*

(6.3.1) $\overline{K}(x)/\overline{K}(f(x))$ *is Galois and* $\deg f$ *is a power of* p.

(6.3.2) $F(X) := f(X) - f(0)$ *is a separable additive polynomial.*

When these conditions hold, the Galois group of $\overline{K}(x)/\overline{K}(f(x))$ *is an elementary abelian* p*-group.*

PROOF. From Lemma 6.2 we get that (6.3.1) and (6.3.2) are equivalent. If both (6.3.1) and (6.3.2) hold, note that $A := \mathrm{Gal}(\overline{K}(x)/\overline{K}(f(x)))$ consists of the automorphisms of $\overline{K}(x)$ which fix $\overline{K}$ and map $x \mapsto x + \alpha$ where $F(\alpha) = 0$; A is hence an elementary abelian p-group of order $\deg f$. □

We use the above characterization of separable additive polynomials to give a short proof of the fact that additive polynomials decompose into additive polynomials. This was first proved by Dorey and Whaples [**25**].

LEMMA 6.4. *Let K be a field of characteristic $p > 0$ and $f \in K[X]$ a separable additive polynomial. If $f = g \circ h$, then $g(X) - g(0)$ and $h(X) - h(0)$ are separable additive polynomials as well.*

PROOF. Let x be transcendental over K. Then by Lemma 6.3 it follows that $\overline{K}(x)/\overline{K}(f(x))$ is Galois with $G := \mathrm{Gal}(\overline{K}(x)/\overline{K}(f(x))$ an elementary abelian p-group. Since $\overline{K}(f(x)) \subseteq \overline{K}(h(x) \subseteq \overline{K}(x)$, it follows that $\overline{K}(x)/\overline{K}(h(x))$ is Galois as well. Since $\deg f$ is a power of p, it follows that $\deg h$ is a power of p as well, so from Lemma 6.3 we get that $h(X) - h(0)$ is separable additive. If we denote $y = h(x)$, then $g(y) = f(x)$ and $\overline{K}(x)/\overline{K}(g(y))$ is hence Galois. Since G is abelian, the subgroup N of G fixing $\overline{K}(y)$ is normal in G, so $\overline{K}(y)/\overline{K}(g(y))$ is Galois. Since $\deg g$ is a power of p, from Lemma 6.3 it follows that $g(X) - g(0)$ is separable additive as well. □

It is further proved in [**25**] that any nonzero additive polynomial (so, not necessarily separable) decomposes into additive polynomials. The argument is very simple and we now quickly recall it.

COROLLARY 6.5. *Let K be a field of characteristic $p > 0$ and $f \in K[X]$ a nonzero additive polynomial. If $f = g \circ h$, then $g(X) - g(0)$ and $h(X) - h(0)$ are additive polynomials as well.*

PROOF. Suppose that there exists a nonzero additive polynomial $f(X)$ such that $f = g \circ h$, but $g(X) - g(0)$ and $h(X) - h(0)$ are not both additive and assume that $f(X)$ is of minimal degree among all such counterexamples. Then $f'(X) = 0$ by Lemma 6.4, so either $g'(X) = 0$ or $h'(X) = 0$. If $h'(X) = 0$, then $f(X) = f_1(X) \circ X^p$ and $h(X) = h_1(X) \circ X^p$ for some $f_1, g_1 \in K[X]$, wherefrom $f_1 = g \circ h_1$, so we have a counterexample of lower degree, a contradiction. Now assume $g'(X) = 0$. Then $f(X) = f_1(X) \circ X^p$ and $g(X) = g_1(X) \circ X^p$, so $f_1(X^p) = g_1(h(X)^p)$. Since $h(X)^p = h_0(X^p)$ for some $h_0 \in K[X]$, it follows that $f_1(X^p) = g_1(h_0(X^p))$, wherefrom $f_1 = g_1 \circ h_0$, which is again a counterexample of lower degree, a contradiction. □

Next we show that the monodromy group of a separable additive polynomial has a transitive abelian subgroup, so that our general results apply to additive polynomials.

LEMMA 6.6. *Let K be a field of characteristic $p > 0$ and let $f \in K[X]$ be separable additive. Then the monodromy group of $f(X)$ has a transitive abelian subgroup.*

PROOF. Let L be the splitting field of $f(X)$ over K. Let t be transcendental over K and let Ω denote the splitting field of $\phi_f(X) = f(X) - t$ over $K(t)$. By Gauss's Lemma it follows that $\phi_f(X)$ is irreducible over $K(t)$. Since $f'(X) \neq 0$,

it follows that $\phi_f(X)$ is separable. Let x be a root of $\phi_f(x)$ in Ω, so $t = f(x)$. For any $\alpha \in L$ such that $f(\alpha) = 0$, we get that $x + \alpha$ is a root of $\phi_f(x)$, since

$$\phi_f(x+\alpha) = f(x+\alpha) - f(x) = f(x) + f(\alpha) - f(x) = f(\alpha) = 0.$$

These are all the roots of $\phi_f(X)$ since $f(X)$ is separable and $\deg \phi_f = \deg f$. So, $\Omega = L(x)$ and $L(x)$ is hence the Galois closure of $K(x)/K(f(x))$. Let G be the monodromy group of $f(X)$, that is $G = \mathrm{Gal}(L(x)/K(f(x))$, and let H be the stabilizer of x in G, so $H = \mathrm{Gal}(L(x)/K(x))$. Let further $A = \mathrm{Gal}(L(x)/L(f(x)))$. Note that A consist of the automorphisms of $L(x)$ that fix L and map $x \mapsto x+\alpha$, where $f(\alpha) = 0$ and is hence an elementary abelian p-group of order $\deg f$. Further note that $A \cap H = 1$, so $|HA| = |H||A| = [L(x) : K(x)] \cdot \deg f = [L(x) : K(x)][K(x) : K(f(x))] = [L(x) : K(f(x)] = |G|$, whence $G = HA$. Since H is the point stabilizer in G, it follows that A is a transitive subgroup of G. □

We are now ready to apply our general results from the previous sections to additive polynomials.

PROPOSITION 6.7. *Let K be a field of characteristic $p > 0$ and let $f(X) \in K[X]$ be separable additive.*

(6.7.1) Any complete decomposition of $f(X)$ can be obtained from any other complete decomposition of $f(X)$ through finitely many steps, where in each step we replace a complete decomposition of $f(X)$ by a Ritt neighbor.

(6.7.2) If $f_1 \circ f_2 \circ \cdots \circ f_m = f = g_1 \circ g_2 \circ \ldots \circ g_n$ are two complete decompositions of $f(X)$ in $K[X]$, then $m = n$ and there is a permutation π of $\{1, 2, \ldots, m\}$ such that $\mathrm{Mon}(f_i) \cong \mathrm{Mon}(g_{\pi(i)})$ for each i. It follows that $\deg f_i = \deg g_{\pi(i)}$ and $\gamma(f_i) = \gamma(g_{\pi(i)})$.

(6.7.3) If $f_1, f_2, \ldots, f_m \in K[X]$ satisfy $f = f_1 \circ f_2 \circ \cdots \circ f_m$, then

$$\gamma(f) \mid \gamma(f_1)\gamma(f_2)\ldots\gamma(f_m).$$

PROOF. From Lemma 6.6 it follows that the monodromy group of $f(x)$ has a transitive abelian subgroup. Now (6.7.1) follows from Theorem 3.2. Proposition 6.4 implies that whenever we replace a complete decomposition with a Ritt neighbor we are replacing two indecomposable polynomials whose composition is an additive polynomial (plus a constant coefficient) by two other indecomposable polynomials with the same composition. Then Theorem 4.1 implies that these pairs of indecomposable polynomials have the same pair of monodromy groups, possibly in reversed order, which proves (6.7.2). Lastly, (6.7.3) follows from Theorem 5.3. □

REMARK 6.8. Ore [**73, 74**] studied additive polynomial decomposition. He proved that the number and the sequence of degrees of indecomposable polynomials in any complete decomposition of a separable additive $f(X)$ is uniquely determined by $f(X)$, up to permutation. Ore's methods are quite different from ours and yield weaker result. At the end of the next section, more words about Ore's methods can be found. We further remark that the proof of Lemma 6.6 is contained in the proof of [**25**, Thm. 4]; this theorem corresponds to our Lemma 6.4. Since Dorey and Whaples followed Ritt's ideas in [**25**], their proof is of similar flavor as ours.

7. Subadditive polynomials

In this section we discuss decompositions of subadditive polynomials, which are defined as follows:

DEFINITION 7.1. For any field K of characteristic $p \geq 0$, a polynomial $S \in K[X]$ is called *subadditive* if $S(X^n) = f(X)^n$ for some separable additive $f(X) \in K[X]$ and some positive integer n for which $p \nmid n$.

We will show that the monodromy group of a subadditive polynomial $S(X)$ over K contains a transitive abelian subgroup, so that the results of the previous sections apply to subadditive polynomials. We do this by showing that the monodromy group of $S(X)$ over a suitable extension of K contains such a subgroup. In fact we prove the following stronger result.

LEMMA 7.2. *Let K be a field of characteristic $p > 0$, and let n be a positive integer coprime to p. Let y be transcendental over K, and put $x := y^n$. For any $g \in K[X] \setminus K[X^p]$, the following are equivalent:*

(7.2.1) $g(X^n) = a(f(X) + c)^n + b$ *for some* $a, b, c \in K$ *and some separable additive* $f(X) \in K[X]$.

(7.2.2) $\overline{K}(y)/\overline{K}(g(x))$ *is Galois and* $\deg g$ *is a power of* p.

When these conditions hold, the Galois group of $\overline{K}(y)/\overline{K}(g(x))$ is the semidirect product of the normal elementary abelian subgroup $\mathrm{Gal}(\overline{K}(y)/\overline{K}(f(y)))$ *and the cyclic subgroup* $\mathrm{Gal}(\overline{K}(y)/\overline{K}(x))$.

PROOF. First assume (7.2.2). By Theorem 6.2, we have $g(X^n) = a(f(X) + c)^n + b$ for some $a, b, c \in \overline{K}$ with $a \neq 0$ and some separable additive $f(X) \in \overline{K}[X]$. In order to obtain (7.2.1), we must show that we can choose a, b, c to be in K and $f(X)$ to be in $K[X]$. First, we may assume that $f(X)$ is monic, upon replacing $(a, c, f(X))$ by $(ad^n, c/d, f(X)/d)$ where d is the leading coefficient of $f(X)$. Then the leading coefficient of $g(X^n)$ equals a, so $a \in K^*$. If $n = 1$ then we may replace (b, c) by $(b + ac, 0)$, so that $g(X) = af(X) + b$; then comparing terms of like degrees shows that $f(X) \in K[X]$ and $b \in K$, so that (7.2.1) holds.

Now suppose $n > 1$, and write $p^k := \deg f$. If $f(X) + c \notin K[X]$, then let $dX^{p^{k-i}}$ be the highest-degree term of $f(X) + c$ which is not in $K[X]$; then the coefficient of $X^{np^{k-i}}$ in $g(X^n)$ is not in K, since $a, c \in K$, a contradiction. Therefore $f(X) + c \in K[X]$, so $f(X) \in K[X]$ and $c \in K$, and thus also $b \in K$. It follows that (7.2.1) holds in every case.

Now assume (7.2.1). Theorem 6.2 implies that $\overline{K}(y)/\overline{K}(g(x))$ is Galois. Moreover, $\deg g = \deg f$ is a power of p, so (7.2.2) holds.

Henceforth assume that both (7.2.1) and (7.2.2) hold. Then in particular, $\overline{K}(y)/\overline{K}(g(x))$ is Galois, so $G := \mathrm{Gal}(\overline{K}(y)/\overline{K}(g(x)))$ has order $[\overline{K}(y) : \overline{K}(g(x))] = [\overline{K}(y) : \overline{K}(x)] \cdot [\overline{K}(x) : \overline{K}(g(x))] = n \cdot \deg g$. Note that $A := \mathrm{Gal}(\overline{K}(y)/\overline{K}(f(y)))$ consists of the automorphisms of $\overline{K}(y)$ which fix $\overline{K}$ and map $y \mapsto y + \alpha$ where $f(\alpha) = 0$, and $H := \mathrm{Gal}(\overline{K}(y)/\overline{K}(x))$ consists of the automorphisms of $\overline{K}(y)$ which fix $\overline{K}$ and map $y \mapsto \zeta x$ where $\zeta^n = 1$. Hence A is elementary abelian of order $\deg f$ (which equals $\deg g$), and H is cyclic of order n. Since $\gcd(n, \deg g) = 1$ we have $A \cap H = 1$, so that $|AH| = |A| \cdot |H| = n \cdot \deg g = |G|$, whence $G = AH$. Pick any $\sigma \in A$ and $\tau \in H$, so that $\sigma(y) = y + \alpha$ and $\tau(y) = \zeta y$ where $f(\alpha) = 0$ and $\zeta^n = 1$. Then $\tau^{-1}\sigma\tau(y) = y + \zeta\alpha$. But since $G = AH$, and the only elements of AH which map $y \mapsto y + \beta$ (with $\beta \in \overline{K}$) are the elements of A, it follows that $\tau^{-1}\sigma\tau \in A$. Therefore H normalizes A, so A is a normal subgroup of G, whence $G = A \rtimes H$. □

We now show that the element c in (7.2.1) must be 0 if $n > 1$, so that the polynomials $g(X)$ in (7.2.1) are obtained from subadditive polynomials by composing with degree-one polynomials.

LEMMA 7.3. *For any field K of characteristic $p \geq 0$, any separable additive $f(X) \in K[X]$, any $a, b, c \in K$ with $a \neq 0$, and any integer $n > 1$ with $p \nmid n$, the following are equivalent:*

(7.3.1) there exists $g(X) \in K[X]$ for which $g(X^n) = a(f(X) + c)^n + b$;
(7.3.2) $c = 0$ and there exists $h(X) \in K[X]$ for which $f(X) = Xh(X^n)$.

When these conditions hold, $g(X)$ and $h(X)$ are uniquely determined, and $g(X) = aXh(X)^n + b$.

PROOF. Suppose that $g(X^n) = a(f(X) + c)^n + b$. If ζ is a primitive n-th root of unity then $g(X^n)$ is unchanged upon replacing X by ζX. Therefore $(f(\zeta X) + c)^n = (f(X) + c)^n$, so that $f(\zeta X) + c = \zeta'(f(X) + c)$ for some n-th root of unity ζ'. It follows that if $f(X) + c$ has a term of degree i then $\zeta^i = \zeta'$. Since $f(X)$ has a term of degree 1, every such i satisfies $\zeta^i = \zeta' = \zeta$, so that $i \equiv 1 \pmod{n}$. Since $n > 1$, it follows that $f(X) + c$ has no term of degree 0, so that $f(X) + c = Xh(X^n)$ for some $h(X) \in K[X]$. Finally, since $f(0) = 0$, we conclude that $c = 0$.

Conversely, if $f(X) = Xh(X^n)$ then plainly $g(X) := aXh(X)^n + b$ satisfies $g(X^n) = af(X)^n + b$. Moreover, both $h(X)$ and $g(X)$ are uniquely determined by the equations $f(X) = Xh(X^n)$ and $g(X^n) = af(X)^n + b$. □

We now use the above results to show that subadditive polynomials can only decompose as the composition of subadditive polynomials. This result was first proved by Henderson and Matthews as the main result of [**57**].

PROPOSITION 7.4. *Let K be a field of characteristic $p > 0$, let n be a positive integer coprime to p, and let $S, f \in K[X] \setminus K[X^p]$ satisfy $S(X^n) = f(X)^n$ where $f(X)$ is additive. For $S_1, S_2 \in K[X]$, we have $S = S_1 \circ S_2$ if and only if there is a degree-one $\mu \in K[X]$ for which $S_1 \circ \mu(X^n) = f_1(X)^n$ and $\mu^{-1} \circ S_2(X^n) = f_2(X)^n$ where $f_1, f_2 \in K[X]$ are separable additive polynomials such that $f = f_1 \circ f_2$.*

PROOF. We may assume that $n > 1$, since if $n = 1$ then the result follows from Theorem 6.4. The "if" direction is easy: if such μ, f_1, f_2 exist, then

$$S_1 \circ S_2(X^n) = S_1 \circ \mu \circ f_2(X)^n = f_1(X)^n \circ f_2(X) = f(X)^n = S(X^n),$$

so $S_1 \circ S_2 = S$. It remains to prove the "only if " direction. Thus, for the rest of this proof we assume that $S = S_1 \circ S_2$. Let y be transcendental over K, and put $x := y^n$. Lemma 7.2 implies that $\overline{K}(y)/\overline{K}(S(x))$ is Galois. Since $\overline{K}(S(x)) \subseteq \overline{K}(S_2(x)) \subseteq \overline{K}(x) \subseteq \overline{K}(y)$, it follows that $\overline{K}(y)/\overline{K}(S_2(x))$ is Galois. Now Lemma 7.2 and Lemma 7.3 imply that $S_2(X^n) = \mu \circ f_2(X)^n$ for some degree-one $\mu \in K[X]$ and some separable additive $f_2(X) \in K[X]$.

By Lemma 7.2, the Galois group G of $\overline{K}(y)/\overline{K}(S(x))$ equals AH where $A := \mathrm{Gal}(\overline{K}(y)/\overline{K}(f(y)))$ and $H := \mathrm{Gal}(\overline{K}(y)/\overline{K}(x))$, and likewise $G_2 := \mathrm{Gal}(\overline{K}(y)/\overline{K}(S_2(x))$ contains $A_2 := \mathrm{Gal}(\overline{K}(y)/\overline{K}(f_2(y)))$. Since $A_2 \subseteq G_2 \subseteq G = AH$, and an element $\sigma \in AH$ satisfies $\sigma(y) - y \in \overline{K}$ if and only $\sigma \in A$, it follows that $A_2 \subseteq A$. Therefore $f(y) = f_1(f_2(y))$ for some $f_1 \in \overline{K}(X)$. Since both $f(x)$ and f_2 are in $K[X]$, also f_1 must be in $K[X]$, so Theorem 6.4 shows that f_1 is additive. Now, writing $\overline{S}_1(X) := S_1(\mu(X))$ and $\overline{S}_2(X) := \mu^{-1}(S_2(X))$, we have

$$f(X)^n = S(X^n) = \overline{S}_1 \circ \overline{S}_2(X^n) = \overline{S}_1 \circ f_2(X)^n.$$

Since both the leftmost and the rightmost expressions are functions of $f_2(X)$, we can equate the corresponding functions to get $f_1(X)^n = \overline{S}_1(X)^n$, which completes the proof. □

REMARK 7.5. Our proof of Proposition 7.4 is completely different from the proof in [**57**], which relied on several pages of computations involving factors of $S(X^n) - S(Y^n)$.

We now apply our general results from the previous sections to the case of subadditive polynomials.

PROPOSITION 7.6. *Let K be a field of characteristic $p > 0$, and let $S(X) \in K[X] \setminus K[X^p]$ be subadditive.*

i) Any complete decomposition of S can be obtained from any other complete decomposition of S through finitely many steps, where in each step we replace a complete decomposition of S by a Ritt neighbor.

ii) If $f_1 \circ f_2 \circ \cdots \circ f_r = S = g_1 \circ g_2 \circ \ldots \circ g_s$ are two complete decompositions of $S(X)$ in $K[X]$, then $r = s$ and there is a permutation π of $\{1, 2, \ldots, r\}$ such that $\mathrm{Mon}(f_i) \cong \mathrm{Mon}(g_{\pi(i)})$ for each i. It follows that $\deg f_i = \deg g_{\pi(i)}$ and $\gamma(f_i) = \gamma(g_{\pi(i)})$.

iii) If $f_1, f_2, \ldots, f_m \in K[X]$ satisfy $S = f_1 \circ f_2 \circ \cdots \circ f_m$, then

$$\gamma(S) \mid \gamma(f_1)\gamma(f_2)\ldots\gamma(f_m).$$

PROOF. All assertions are vacuously true if $\deg S = 1$, so we assume henceforth that $\deg S > 1$. We first show that the monodromy group $\mathrm{Mon}(S)$ of $S(X)$ over K contains a transitive abelian subgroup. Write $S(X^n) = f(X)^n$ where $f(X) \in K[X] \setminus K[X^p]$ is additive and n is a positive integer coprime to p. Let y be transcendental over K, and put $x := y^n$. Proposition 7.2 shows that $\overline{K}(y)/\overline{K}(S(x))$ is Galois, and its Galois group G equals AH where A and H are the Galois groups of $\overline{K}(y)/\overline{K}(f(y))$ and $\overline{K}(y)/\overline{K}(x)$, both of which are abelian. Note that H contains no nontrivial normal subgroup of G: for, any $\tau \in H \setminus \{1\}$ and $\sigma \in A \setminus \{1\}$ satisfy $\tau(y) = \zeta y$ and $\sigma(y) = y + \alpha$ where $\alpha \neq 0$ and $\zeta \neq 1$, so that $\sigma^{-1}\tau\sigma$ maps $y \mapsto \zeta y + \alpha(1 - \zeta) \notin \overline{K}^* y$, whence $\sigma^{-1}\tau\sigma \notin H$. It follows that $\overline{K}(y)$ is the Galois closure of the extension of fixed fields $\overline{K}(y)^H/\overline{K}(y)^G$, or equivalently of $\overline{K}(x)/\overline{K}(S(x))$. Since H is the subgroup of G which fixes x, the factorization $G = HA$ shows that the abelian subgroup A of G acts transitively on the conjugates of x over $\overline{K}(S(x))$, or equivalently, on the roots of $S(X) - S(x)$. Now let Ω be the Galois closure of $K(x)/K(S(x))$. Then $\Omega \subseteq K(y)$, and restricting elements of G to Ω induces an isomorphism of G onto $\mathrm{Gal}(\Omega/L(S(x)))$, where $L := \Omega \cap \overline{K}$. In particular, G is isomorphic as a permutation group to a subgroup of $\mathrm{Mon}(S)$, so since G has a transitive abelian subgroup, it follows that $\mathrm{Mon}(S)$ does as well.

Now (7.6.1) follows from Theorem 3.2. Proposition 7.4 implies that if $S = h_1 \circ h_2 \circ \cdots \circ h_m$ where each $h_i \in K[X]$, then $h_i \circ h_{i+1} = \mu \circ S_i \circ \nu$ where $S_i \in K[X]$ is subadditive and $\mu, \nu \in K[X]$ have degree one. Therefore whenever we replace a complete decomposition of S by a Ritt neighbor, we are replacing two indecomposable polynomials whose composition is subadditive (composed with linears) by two other indecomposable polynomials having the same composition. It follows from Theorem 4.1 that these two pairs of indecomposable polynomials have the same pair of monodromy groups, possibly in reversed order. This implies (7.6.2). Finally, (7.6.3) follows from Theorem 5.3. □

REMARK 7.7. The only part of this result which has been stated previously is the assertion that any two complete decompositions of a subadditive polynomial have the same length and the same sequence of degrees of indecomposables, up to permutation. This assertion occurs on [**21**, p. 325], together with a two-sentence sketch of the proof strategy. Essentially they argue that, in light of Proposition 7.4 and Lemma 7.3, this assertion reduces to showing the analogous properties for expressions of members of a certain subclass Λ of additive polynomials as compositions of members of Λ. Specifically, Λ consists of those additive polynomials in which all terms have degree congruent to 1 mod p^k, where $\mathbf{F}_{p^k}$ is the extension of $\mathbf{F}_p$ obtained by adjoining all n-th roots of unity. The relevant properties of members of Λ were proved by Ore [**74**, Thm. 1 of Chap. II, p. 494]. We note that Ore's proof is completely different from ours. In particular, while both proofs show that any complete decomposition of an additive polynomial can be obtained from any other such decomposition through finitely many steps, our steps involve replacing two adjacent indecomposables by two others having ths same composition, whereas Ore's steps replace a block of $r \geq 2$ consecutive indecomposables by another block of r indecomposables which have the same composition, where the degrees of the second batch of indecomposables are a circular shift of the degrees of the first batch of indecomposables. Moreover, Ore does not use Galois closures or monodromy groups, so his methods do not give information about the other parts of Proposition 7.6.

Chapter 3

Diophantine equations with Euler polynomials

This chapter contains the paper [**59**] with the title *Diophantine equations with Euler polynomials*. It is a joint paper with Csaba Rakaczki. The article was published in *Acta Arithmetica* in 2013. The presentation of the paper here is slightly modified from the published version of the paper.

Abstract. In this paper we determine possible decompositions of Euler polynomials $E_k(x)$, i.e. possible ways of writing Euler polynomials as a functional composition of polynomials of lower degree. Using this result together with the well-known criterion of Bilu and Tichy, we prove that the Diophantine equation

$$-1^k + 2^k - \cdots + (-1)^x x^k = g(y),$$

with $\deg g \geq 2$ and $k \geq 7$, has only finitely many integers solutions x, y unless polynomial g can be decomposed in ways that we list explicitly.

1. Introduction

If K is a field and $g(x), h(x) \in K[x]$, then $f = g \circ h$ is a functional composition of g and h and (g, h) is a (functional) *decomposition* of f (over K). The decomposition is *nontrivial* if g and h are of degree at least 2. A polynomial is said to be *indecomposable* if it is of degree at least 2 and does not have a nontrivial decomposition. Given $f(x) \in K[x]$ with $\deg f > 1$, a *complete decomposition* of f is a decomposition $f = f_1 \circ f_2 \cdots \circ f_m$, where polynomials $f_i \in K[x]$ are indecomposable for all $i = 1, 2, \ldots, m$. Two decompositions $f = g_1 \circ h_1 = g_2 \circ h_2$ are said to be *equivalent* over K if there exists a linear polynomial $\ell \in K[x]$ such that $g_2 = g_1 \circ \ell$ and $h_1 = \ell \circ h_2$. Complete decomposition of a polynomial of degree greater than 1 clearly always exists, but it does not need to be unique. In 1922, J. F. Ritt [**84**] proved that any two complete decomposition of $f \in \mathbb{C}[x]$ consist

of the same number of indecomposable polynomials and moreover that the sequence of degrees of polynomials in a complete decomposition of f is uniquely determined by f, up to permutation. This result is known in literature as Ritt's first theorem. For more on the topic of polynomial decomposition we refer to [**89**].

Ritt's polynomial decomposition results have been applied to a variety of topics. One such topic is the classification of polynomials f and g with rational coefficients such that the equation $f(x) = g(y)$ has infinitely many integer solutions. In 2000, Bilu and Tichy [**13**] presented a complete and definite answer to this question. In the past decade the theorem of Bilu and Tichy has been applied to various Diophantine equations. For example, in [**12**] it is shown that the equation $1^m+2^m+\cdots+x^m = 1^n+2^n+\cdots+y^n$ has only finitely many integer solutions x, y, provided $m, n \geq 2$ and $m \neq n$. In [**80**] Rakaczki investigated the question of the finiteness of the number of integer solutions x, y of the equation $1^m + 2^m + \cdots + x^m = g(y)$ with an arbitrary $g(x) \in \mathbb{Q}[x]$. We mention that the study of Diophantine equations involving power sums of consecutive integers has a long history, dating back to the work of Schäffer in 1956, see [**87**]. In the present paper we study a related problem.

The purpose of this paper is to characterize those $g \in \mathbb{Q}[x]$ for which the Diophantine equation

$$-1^k + 2^k - \cdots + (-1)^x x^k = g(y) \tag{1.1}$$

has infinitely many integer solutions. It is well known, see for instance [**1**], that the following relation holds:

$$-1^k + 2^k - 3^k + \cdots + (-1)^n n^k = \frac{E_k(0) + (-1)^n E_k(n+1)}{2},$$

where $E_k(x)$ denotes the k-th Euler polynomial, which is defined by the following generating function:

$$\sum_{k=0}^{\infty} E_k(x)\frac{t^k}{k!} = \frac{2\exp(tx)}{\exp(t)+1}.$$

In the present paper we give a complete description of decompositions of Euler polynomials into polynomials with complex coefficients.

THEOREM 1.2. *Euler polynomials $E_k(x)$ are indecomposable for all odd k. If $k = 2m$ is even, then every nontrivial decomposition of $E_k(x)$ over complex numbers is equivalent to*

$$E_k(x) = \widetilde{E}_m\left(\left(x-\frac{1}{2}\right)^2\right), \text{ where } \widetilde{E}_m(x) = \sum_{j=0}^{m}\binom{2m}{2j}\frac{E_{2j}}{4^j}x^{m-j} \tag{1.3}$$

and E_j is the j-th Euler number defined by $E_j = 2^j E_j(1/2)$. In particular, the polynomial $\widetilde{E}_m(x)$ is indecomposable for any $m \in \mathbb{N}$.

Since Euler polynomials appear in many classical results and play an important role in various approximation and expansion formulas in discrete mathematics and in number theory (see for instance [**1, 15**]), we find that Theorem 1.2 might be of broader interest. Theorem 1.2 together with the aforementioned criterion of Bilu and Tichy allows us to prove the following theorem.

THEOREM 1.4. *Let $k \geq 7$ be an integer and $g(x) \in \mathbb{Q}[x]$ with $\deg g \geq 2$. Then the Diophantine equation* (1.1) *has only finitely many integer solutions unless we are in one of the following cases*

$$\begin{aligned}
&\textit{i)}\ g(x) = f\left(E_k(p(x))\right),\\
&\textit{ii)}\ g(x) = f\left(\widetilde{E}_s\left(p(x)^2\right)\right),\\
&\textit{iii)}\ g(x) = f\left(\widetilde{E}_s\left(\delta(x)p(x)^2\right)\right),\\
&\textit{iv)}\ g(x) = f\left(\widetilde{E}_s\left(\gamma\delta(x)^t\right)\right),\\
&\textit{v)}\ g(x) = f\left(\widetilde{E}_s\left(\left(a\delta(x)^2+b\right)p(x)^2\right)\right),
\end{aligned}$$

where $a, b, \gamma \in \mathbb{Q}\backslash\{0\}$, $t \geq 3$ odd, $E_k(x)$ is the k-th Euler polynomial, $p(x) \in \mathbb{Q}[x]$, $\delta(x) \in \mathbb{Q}[x]$ is a linear polynomial,

$$f(x) = \pm\frac{x}{2} + \frac{E_k(0)}{2} \quad \text{and} \quad \widetilde{E}_s(x) = \sum_{j=0}^{s} \binom{2s}{2j} \frac{E_{2j}}{4^j} x^{s-j}.$$

The proof of Theorem of Bilu and Tichy relies on Siegel's classical theorem on integral points on curves, which is ineffective. Consequently, the Theorem 1.4 is ineffective.

In the proof of Theorem 1.4 in each of the exceptional cases, we find an infinite family of integer solutions of the equation (1.1).

In relation to our problem we mention a paper by Dilcher [**24**], where the effective finiteness theorem is established for the Diophantine equation

$$-1^k + 3^k - \cdots - (4x-3)^k + (4x-1)^k = y^n, \tag{1.5}$$

which was viewed as a "character-twisted" analogue of Schäffer's equation [**87**], and a recent paper by Bennett [**10**], where the same equation was completely solved for $3 \leq k \leq 6$ using methods from Diophantine approximations, as well as techniques based upon the modularity of Galois representations. Using our techniques, one can obtain ineffective finiteness theorems of a similar flavor as Theorem 1.4 for the Diophantine equation

$$-1^k + 3^k - \cdots - (4x-3)^k + (4x-1)^k = g(y), \tag{1.6}$$

with $k \in \mathbb{N}$ and an arbitrary $g(x) \in \mathbb{Q}[x]$.

2. Decomposition of Euler polynomials

In this section we recall and establish some results on polynomial decomposition and then use them to determine decomposition properties of Euler polynomials.

The following lemma describes the structure of the set of all decompositions of a fixed monic polynomial into two decomposition factors in the case when the corresponding field is either of characteristic 0 or of positive characteristic, but the degree of the polynomial is not divisible by the characteristic of the field. This case is known in literature as the *tame case*. In the tame case, there are known analogues of Ritt's theorems. The case in which the degree of the polynomial is divisible by the characteristic of the field is called *wild* and in this case analogues of Ritt's results do not hold, see [**25**]. Similarly, the following lemma also fails in wild case.

LEMMA 2.1. *Let $f(x) \in K[x]$ be a monic polynomial such that* $\operatorname{char}(K) \nmid \deg f$. *Let L be an arbitrary extension field of K. Then for any nontrivial decomposition $f = f_1 \circ f_2$ with $f_1(x), f_2(x) \in L[x]$, there exists a unique decomposition $f = \tilde{f}_1 \circ \tilde{f}_2$, such that the following conditions are satisfied:*

i) $\tilde{f}_1(x)$ and $\tilde{f}_2(x)$ are monic polynomials with coefficients in K,
ii) $\tilde{f}_1 \circ \tilde{f}_2$ and $f_1 \circ f_2$ are equivalent over L,
iii) if we denote $t := \deg \tilde{f}_1$, then the coefficient of x^{t-1} in $\tilde{f}_1(X)$ is 0.

PROOF. Let $f(x) = f_1(f_2(x))$ be a nontrivial decomposition of $f(x) \in K[x]$ with $f_1(x), f_2(x) \in L[x]$. Let $t = \deg f_1$, $k = \deg f_2$ and let $b_k \in L$ be the leading coefficient of $f_2(x)$. Then

$$\hat{f}_1(x) := f_1(b_k x), \quad \hat{f}_2(x) := b_k^{-1} f_2(x)$$

are clearly monic polynomials. Let $\hat{a}_{t-1}$ be the coefficient of x^{t-1} in $\hat{f}_1(x)$. Let

$$\tilde{f}_1(x) := \hat{f}_1(x - t^{-1}\hat{a}_{t-1}), \quad \tilde{f}_2(x) := \hat{f}_2(x) + t^{-1}\hat{a}_{t-1}.$$

It is easy to verify that the coefficient of x^{t-1} in $\tilde{f}_1(x)$ is 0 and since $\hat{f}_1$ and $\hat{f}_2$ are monic, so are $\tilde{f}_1$ and $\tilde{f}_2$. Let $\tilde{f}_1(x) = x^t + a_{t-1}x^{t-1} + \cdots + a_0$ and $\tilde{f}_2(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0$, where $a_i, b_j \in L$, for $i = 0, 1, \ldots, t$, $j = 0, 1, \ldots, k$, and $a_{t-1} = 0$. Further let $f(x) = c_n x^n + \cdots + c_1 x + c_0$. Now we can easily see that $\tilde{f}_1$ and $\tilde{f}_2$ are uniquely determined and have coefficients in K. From

$$f(x) = \tilde{f}_1(\tilde{f}_2(x)) = \tilde{f}_2(x)^t + a_{t-2}\tilde{f}_2(x)^{t-2} + \cdots + a_1\tilde{f}_2(x) + a_0, \tag{2.2}$$

by expanding $\tilde{f}_2(x)^t$ we get the following system of equations which completely determine coefficients of $\tilde{f}_2(x)$:

$$\begin{cases} c_{n-1} = tb_{k-1} \\ c_{n-2} = tb_{k-2} + \binom{t}{2} b_{k-1}^2 \\ \qquad \vdots \\ c_{n-k} = tb_0 + \sum\limits_{i_1+2i_2+\cdots+(k-1)i_{k-1}=k} d_{i_1,i_2,\ldots,i_{k-1}}\ b_{k-1}^{i_1} b_{k-2}^{i_2} \ldots b_1^{i_{k-1}}, \end{cases} \tag{2.3}$$

where

$$d_{i_1,i_2,\ldots,i_{k-1}} = \binom{t}{i_1, i_2, \ldots, i_{k-1}}.$$

Since $c_i \in K$, it follows that $b_i \in K$ for all $i = 0, 1, \ldots, k-1$ and hence $\tilde{f}_2(x) \in K[x]$. Furthermore, from (2.2) it follows that the coefficients of $\tilde{f}_1$ are uniquely determined by F and $\tilde{f}_2$. Recursively, $a_i \in K$ for all $i = t-2, \ldots, 1, 0$. Hence, $\tilde{f}_1(x) \in K[x]$ as well. □

The proof of Lemma 2.1 fails when the degree of the polynomial is divisible by the characteristic of the field, since in this case there does not exist the multiplicative inverse of the degree of the polynomial in the field.

Lemma 2.1 implies that if $f \in K[x]$ is indecomposable over K, then it is indecomposable over any extension field of K, provided $\operatorname{char}(K) \nmid \deg f$. This result is well known. In fact, we built up a proof of Lemma 2.1 based on [**?**, Theorem 6, Chapter 1.3].

We will further need the following lemma.

LEMMA 2.4. *Let $f \in K[x]$ such that $\operatorname{char}(K) \nmid \deg f$. If $f = g_1 \circ g_2 = h_1 \circ h_2$ and $\deg g_1 = \deg h_1$, and hence $\deg g_2 = \deg h_2$, then there exists a linear polynomial $\ell \in K[x]$ such that $g_1(x) = h_1(\ell(x))$ and $h_2(x) = \ell(g_2(x))$.*

PROOF. The case $K = \mathbb{C}$ is contained already in [**84**]. Lemma was later proved in generality by Levi [**65**]. □

The following observation will be of great help to the proof.

LEMMA 2.5. *Let n be an even positive integer. If*

$$(x+1)^n - x^n = g(x)h(x)$$

with $g(x), h(x) \in \mathbb{R}[x]$, then the coefficients of $g(x)$ and $h(x)$ are either all positive or all negative.

PROOF. We have $(x+1)^n - x^n = \prod_{i=1}^{n}(x + 1 - \omega_i x)$, where $\omega_i = e^{\frac{2\pi i}{n}}$, $i = 1, 2, \ldots, n$. Let $n = 2k$. Hence, $\omega_{2k} = 1$, $\omega_k = -1$, and $\omega_{2k-j} = \overline{\omega_j}$ for all

$j = 1, 2, \ldots, k-1$. Therefore we have

$$\begin{aligned}(x+1)^n - x^n &= (2x+1)\prod_{j=1}^{k-1}(x+1-\omega_j x)\,(x+1-\overline{\omega_j}x)\\ &= (2x+1)\prod_{j=1}^{k-1}\left((2-(\omega_j+\overline{\omega_j}))x^2+(2-(\omega_j+\overline{\omega_j}))x+1\right).\end{aligned}$$

Clearly $2-(\omega_j+\overline{\omega_j})>0$ for all $j\in\{1,2,\ldots,k-1\}$. Now the assertion follows from the fact that the ring $\mathbb{R}[x]$ is a unique factorization domain. □

We will make an extensive use of the following theorem of Rakaczki [**81**].

THEOREM 2.6. *Let $m \geq 7$ be an integer. Then the polynomial $E_m(x)+b$ has at least three simple zeros for arbitrary complex number b.*

Finally, to the proof of Theorem 1.2 we need the following proposition, in which we collect some well known properties of Euler polynomials, which will be used in the sequel, sometimes without particular reference, see [**15**] for proofs.

PROPOSITION 2.7.

i) $E_n(x) = (-1)^n E_n(1-x)$;

ii) $E_n(x+1) + E_n(x) = 2x^n$;

iii) $E_n'(x) = nE_{n-1}(x)$;

iv) $E_5(x)$ *is the only Euler polynomial with a multiple root.*

v) If E_k denotes the k-th Euler number, which is defined by $E_k = 2^k E_k(1/2)$, then

$$E_n(x) = \sum_{k=0}^{n}\binom{n}{k}\frac{E_k}{2^k}\left(x-\frac{1}{2}\right)^{n-k},$$

i.e. $E_n(x) = \sum_{k=0}^{n} c_k x^k$ with

$$c_k = \sum_{j=0}^{n-k}\binom{n}{j}\frac{E_j}{2^j}\binom{n-j}{k}\left(\frac{-1}{2}\right)^{n-k-j},$$

for $k = 0, 1, \ldots, n$. In particular,

$$c_n = 1,\ c_{n-1} = -\frac{1}{2}n,\ c_{n-2} = 0,\ c_{n-3} = \frac{1}{4}\binom{n}{3},\ \text{etc.}$$

PROOF OF THEOREM 1.2. Let $n \in \mathbb{N}$ and

$$E_n(x) = g(h(x)) \tag{2.8}$$

be a nontrivial decomposition of the n-th Euler polynomial. By Lemma 2.1 we may assume that polynomials $g(x)$ and $h(x)$ are monic with rational coefficients; let $g(x) = x^t + a_{t-1}x^{t-1} + \cdots + a_0 \in \mathbb{Q}[x]$ and $h(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0 \in \mathbb{Q}[x]$. By the same lemma we may assume $a_{t-1} = 0$. Note $t, k \geq 2$ by assumption.

Using (2.3) we can express the coefficients of $h(x)$ in terms of coefficients of the $E_n(x)$, which are given in Proposition 2.7, so

$$b_{k-1} = -\frac{k}{2}, \quad b_{k-2} = -\frac{(t-1)k^2}{8}, \tag{2.9}$$
$$b_{k-3} = \frac{1}{4}\binom{k}{3} + \frac{(t-1)k^2(k-2)}{16}.$$

From $E_n(1-x) = (-1)^n E_n(x)$, it follows that

$$g(h(1-x)) = (-1)^n g(h(x)). \tag{2.10}$$

We first consider the case when n is even. Then $g(h(1-x)) = g(h(x))$. From Lemma 2.4, by using $a_{t-1} = 0$, we get that either $h(1-x) = h(x)$ or $h(1-x) = -h(x)$ and $g(x) = g(-x)$. In the former case k is even. From Proposition 2.7 we get

$$2\left((x+1)^n - x^n\right) = E_n(-x-1) - E_n(x) = g(h(-x-1)) - g(h(x)),$$

so $(x+1)^n - x^n$ is divisible by $h(-x-1) - h(x)$ in $\mathbb{Q}[x]$. Note that the leading coefficient of $h(-x-1) - h(x)$ is $k - 2b_{k-1} = 2k$. If $k \geq 4$, from Lemma 2.5 it follows that the coefficient of x^{k-4} in $h(-x-1) - h(x)$ is positive, so

$$\binom{k}{4} - \binom{k-1}{3} b_{k-1} + \binom{k-2}{2} b_{k-2} - \binom{k-3}{1} b_{k-3} > 0. \tag{2.11}$$

Using (2.9) we obtain

$$\binom{k}{4} > \frac{(t-1)k^2(k-2)(k-3)}{16},$$

wherefrom $t \leq 1$, contradicting the assumption. Since k is even, we conclude $k = 2$ and hence $n = 2t$. Lemma 2.4 implies that this decomposition is equivalent to the decomposition (1.3).

In the case when $h(1-x) = -h(x)$ and $g(x) = g(-x)$ one can deduce that k is odd, t is even, $g(x) = x^t + a_{t-2}x^{t-2} + \cdots + a_2x^2 + a_0$ and

$$E_n(x) = g(h(x)) = g_1(h_1(x)),$$

where

$$g_1(x) = x^{t/2} + a_{t-2}x^{t/2-1} + \cdots + a_2x + a_0, \quad h_1(x) = h(x)^2.$$

But then $h_1(x) = h_1(1-x)$ and we can use the argument above to get a contradiction provided $t \geq 4$. If $t = 2$, then $g(x) = x^2 + a_0$ and hence $E_n(x) = h(x)^2 + a_0$. From Theorem 2.6 it follows that this is possible only when $n \leq 6$. Since $n \geq 4$ and k is odd, it follows that the only possibility is $n = 6$, but a direct calculation shows that $E_6(x)$ is not of this form.

If n is odd, then k and t are also odd. Proposition 2.7 implies

$$2x^n = E_n(x) - E_n(-x) = g(h(x)) - g(h(-x)),$$

wherefrom we deduce that $h(x) - h(-x)$ divides $2x^n$ in $\mathbb{Q}[x]$. Hence, $h(x) - h(-x) = qx^l$ with $q \in \mathbb{Q}$ and $l \leq n$. By expanding $h(x) - h(-x)$ we obtain $l = k$, $q = 2$ and $b_{k-2} = 0$, which together with (2.9) implies $t = 1$ or $k = 0$, contradicting the assumption $k, t \geq 2$. Hence, Euler polynomials with odd index are indecomposable. □

3. Application of the theorem of Bilu and Tichy

To the proof of Theorem 1.4 we need some auxiliary results. First we recall the finiteness criterion of Bilu and Tichy [**13**].

We say that the equation $f(x) = g(y)$ has infinitely many *rational solutions with a bounded denominator* if there exists a positive integer λ such that $f(x) = g(y)$ has infinitely many rational solutions x, y satisfying $\lambda x, \lambda y \in \mathbb{Z}$. If the equation $f(x) = g(y)$ has only finitely many rational solutions with a bounded denominator, then it clearly has only finitely many integer solutions.

We further need to define five kinds of so-called *standard pairs* of polynomials.

In what follows a and b are nonzero rational numbers, m and n are positive integers, $r \geq 0$ is an integer and $p(x) \in \mathbb{Q}[x]$ is a nonzero polynomial (which may be constant).

A *standard pair over* $\mathbb{Q}$ *of the first kind* is $(x^m, ax^r p(x)^m)$, or switched, i.e $(ax^r p(x)^m, x^m)$, where $0 \leq r < m$, $\gcd(r, m) = 1$ and $r + \deg p > 0$.

A *standard pair over* $\mathbb{Q}$ *of the second kind* is $\left(x^2, \left(ax^2 + b\right) p(x)^2\right)$, or switched.

Denote by $D_m(x, a)$ the m-th Dickson polynomial with parameter a, defined by the functional equation

$$D_m\left(x + \frac{a}{x}, a\right) = x^m + \left(\frac{a}{x}\right)^m$$

or by the explicit formula

$$D_m(x, a) = \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-a)^i x^{m-2i}. \tag{3.1}$$

A *standard pair over* $\mathbb{Q}$ *of the third kind* is $\left(D_m\left(x, a^n\right), D_n\left(x, a^m\right)\right)$, where $\gcd(m, n) = 1$.

A *standard pair over* $\mathbb{Q}$ *of the fourth kind* is

$$\left(a^{-m/2} D_m(x, a), -b^{-n/2} D_n(x, b)\right),$$

where $\gcd(m, n) = 2$.

A *standard pair over* $\mathbb{Q}$ *of the fifth kind* is $\left(\left(ax^2 - 1\right)^3, 3x^4 - 4x^3\right)$, or switched.

THEOREM 3.2. *Let $f(x)$ and $g(x)$ be non-constant polynomials in $\mathbb{Q}[x]$. Then the following assertions are equivalent.*

- *The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator;*
- *We have*

$$f(x) = \varphi\left(f_1\left(\lambda(x)\right)\right), \quad g(x) = \varphi\left(g_1\left(\mu(x)\right)\right),$$

where $\lambda(x)$ and $\mu(x)$ are linear polynomials in $\mathbb{Q}[x]$, $\varphi(x) \in \mathbb{Q}[x]$, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.

The following theorem for hyperelliptic equations is due to Baker [**2**].

THEOREM 3.3. *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial with at least three simple roots. Then all the integer solutions of the equation $f(x) = y^2$ satisfy $\max\{|x|, |y|\} \leq C$, where C is an effectively computable constant that depends only on the coefficients of f.*

For $P(x) \in \mathbb{C}[x]$, a complex number c is said to be an *extremum* if $P(x) - c$ has multiple roots. If $P(x) - c$ has s multiple roots, the *type* of c is the tuple $(\alpha_1, \alpha_2, \ldots, \alpha_s)$ of multiplicities of its roots in an increasing order. Clearly $s < \deg P$, $(\alpha_1, \alpha_2, \ldots, \alpha_s) \neq (1, 1, \ldots, 1)$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_s = \deg P$.

In what follows $D_k(x, a)$ denotes the Dickson polynomial of degree $k \in \mathbb{N}$ with parameter $a \in \mathbb{Q} \setminus \{0\}$. The following result on Dickson polynomials can be found in [**11**, Proposition 3.3].

THEOREM 3.4. *If $k \geq 3$, then $D_k(x, a)$ has exactly two extrema and those are $\pm 2a^{\frac{k}{2}}$. If k is odd, then both are of type (1,2,2,...,2). If k is even, then $2a^{\frac{k}{2}}$ is of type (1,1,2,...,2) and $-2a^{\frac{k}{2}}$ is of type (2,2,...,2).*

What follows is a technical lemma which will be needed in the proof of Theorem 1.4.

LEMMA 3.5. *The polynomial $E_n(cx + d)$ is neither of the form $ux^q + v$ with $q \geq 3$, nor of the form $uD_k(x, a) + v$ with $k > 4$, where $c, u \in \mathbb{Q} \setminus \{0\}$, $d, v \in \mathbb{Q}$.*

PROOF. Suppose $E_n(cx + d) = ux^q + v$ with $q \geq 3$, so $q = n$. It follows that the polynomial $(E_n(cx + d) - v)' = ncE_{n-1}(cx + d)$ has a zero with multiplicity $n - 1$. This is not possible, see Proposition 2.7. Now assume that $E_n(cx + d) = uD_k(x, a) + v$ and $n \geq 7$. So, $k = n$ and

$$D_n(x, a) \pm 2a^{\frac{n}{2}} = \frac{1}{u}\left(E_n(cx + d) - v \pm 2ua^{\frac{n}{2}}\right).$$

Then from Theorem 2.6 it follows that $D_n(x,a) \pm 2a^{\frac{n}{2}}$ has at least three simple zeros, which contradicts Theorem 3.4. In the case when $n = 5$ and $n = 6$, a direct calculation shows that $E_n(cx+d)$ is not of the form $uD_n(x,a)+v$. We remark that

$$E_4\left(cx+\frac{1}{2}\right) = c^4 D_4\left(x, \frac{3}{8c^2}\right) + \frac{1}{32}.$$

□

Proof of Theorem 1.4. We recall

$$-1^k + 2^k + \cdots + (-1)^n n^k = \frac{E_k(0) + (-1)^n E_k(n+1)}{2}.$$

Therefore, the study of integer solutions of the equation (1.1) reduces to the study of solutions of the equations

$$\frac{E_k(0) + E_k(2x+1)}{2} = g(y) \tag{3.6}$$

$$\frac{E_k(0) - E_k(2x)}{2} = g(y). \tag{3.7}$$

in integers x, y with x positive. We can study these two equations at once by writing

$$f(E_k(h(x))) = g(y), \tag{3.8}$$

where the equation (3.6) corresponds to polynomials

$$f(x) = \frac{E_k(0)+x}{2}, \quad h(x) = 2x+1, \tag{3.9}$$

and the equation (3.7) to polynomials

$$f(x) = \frac{E_k(0)-x}{2}, \quad h(x) = 2x. \tag{3.10}$$

We further denote

$$F_k(x) = f(E_k(h(x))). \tag{3.11}$$

If $\deg g = 2$, then the equation (3.8) can be re-written as

$$df(E_k(h(x))) = ay^2 + by + c$$

with $a, b, c, d \in \mathbb{Z}$, $a, d \neq 0$, which can be transformed into

$$uE_k(h(x)) + v = (2ay+b)^2, \tag{3.12}$$

where $u, v \in \mathbb{Q}$ and $u \neq 0$. From Theorem 3.3 and Theorem 2.6, we get that the equation (3.12) has only finitely many integer solutions x, y, which can be effectively determined, since $k \geq 7$ by assumption.

Let $\deg g > 2$. Suppose that the equation (3.8) has infinitely many integer solutions. By Theorem 3.2 there exists $\varphi(x) \in \mathbb{Q}[x]$, linear polynomials

$\lambda(x), \mu(x) \in \mathbb{Q}[x]$ and a standard pair $(f_1(x), g_1(x))$ over $\mathbb{Q}$ such that

$$F_k(x) = \varphi(f_1(\lambda(x))), \quad g(x) = \varphi(g_1(\mu(x))). \tag{3.13}$$

Then from Theorem 1.2 and (3.11) we get that either $\deg \varphi = k$ or $\deg \varphi = 1$ or $\deg \varphi = k/2$.

Consider the case $\deg \varphi = k$. Then from (3.13) we get $\deg f_1 = 1$, so $F_k(x) = \varphi(t(x))$, where $t(x) \in \mathbb{Q}[x]$ is a linear polynomial. Then clearly

$$F_k\left(t^{\langle -1\rangle}(x)\right) = \varphi(x),$$

wher $t^{\langle -1\rangle}$ denotes the inverse of t with respect to functional composition. Then from (3.13) we get

$$g(x) = \varphi(g_1(\mu(x))) = F_k\left(t^{\langle -1\rangle}\left(g_1(\mu(x))\right)\right),$$

that is

$$g(x) = f(E_k(p(x))) \tag{3.14}$$

with $p(x) = h\left(t^{\langle -1\rangle}\left(g_1(\mu(x))\right)\right) \in \mathbb{Q}[x]$. In this particular case the equation (3.8) turns into

$$f(E_k(h(x))) = f(E_k(p(y)). \tag{3.15}$$

If we let $r(x) \in \mathbb{Q}[x]$ be an integer valued polynomial which attains only positive values and $p(x) = h(r(x))$, then the equation (3.15) clearly has infinitely many positive integer solutions.

Consider the case $\deg \varphi = 1$. Let $\varphi(x) = \varphi_1 x + \varphi_0$, where $\varphi_1, \varphi_0 \in \mathbb{Q}$ and $\varphi_1 \neq 0$. From (3.13) it follows that

$$F_k\left(\lambda^{\langle -1\rangle}(x)\right) = \varphi(f_1(x)) = \varphi_1 f_1(x) + \varphi_0$$

and from (3.11) it follows that

$$f\left(E_k\left(h\left(\lambda^{\langle -1\rangle}(x)\right)\right)\right) = F_k\left(\lambda^{\langle -1\rangle}(x)\right) = \varphi_1 f_1(x) + \varphi_0.$$

Since $f(x), h(x), \lambda^{\langle -1\rangle}(x) \in \mathbb{Q}[x]$ are linear polynomials, we have that

$$E_k(cx + d) = u f_1(x) + v \tag{3.16}$$

for some $c, d, u, v \in \mathbb{Q}$, $c, u \neq 0$. Next we study five kinds of standard pairs of polynomials over $\mathbb{Q}$.

First consider the case when $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ of the first kind. From (3.16) we get that either $E_k(cx + d) = ux^t + v$ or $E_k(cx + d) = uax^r q(x)^t + v$, where $0 \leq r < t$, $(r, t) = 1$ and $r + \deg q > 0$. In the former case we get a contradiction by Lemma 3.5, since by assumption $k = t \geq 7$. In the latter case, from Theorem 2.6 we get $t \leq 2$, contradiction.

Let now $(f_1(x), g_1(x))$ be a standard pair over $\mathbb{Q}$ of the second kind. Then either $E_k(cx+d) = ux^2 + v$ or $E_k(cx+d) = u\left(ax^2+b\right) q(x)^2 + v$. The former case is not possible since $k \geq 7$ and the latter case is not possible by Theorem 2.6.

Next let $(f_1(x), g_1(x))$ be a standard pair of the third or of the fourth kind. Then by (3.16) it follows that

$$E_k(cx+d) = uD_k(x,w) + v,$$

where $w = a^t$ or $w = a$. Since $k \geq 7$ by assumption, we have a contradiction with Lemma 3.5

Finally, $(f_1(x), g_1(x))$ can not be a standard pair over $\mathbb{Q}$ of the fifth kind since $k \geq 7$.

Finally, consider the case $\deg \varphi = k/2$. Then $k = 2s$ and $\deg f_1 = 2$. From (3.11) and (3.13) we get

$$E_k(x) = f^{\langle -1 \rangle}\left(\varphi(f_1(\tau(x)))\right), \tag{3.17}$$

where $\tau(x)$ is a linear polynomial in $\mathbb{Q}[x]$. Since $\deg f_1 = 2$ and $k \geq 7$, we have a nontrivial decomposition of $E_k(x)$ in (3.17). From Theorem 1.2 it follows that there exists a linear polynomial $u(x)$ such that

$$\varphi(x) = f\left(\widetilde{E}_s\left(u(x)\right)\right), \quad u\left(f_1(\tau(x))\right) = \left(x - \frac{1}{2}\right)^2, \tag{3.18}$$

which together with (3.13) implies

$$g(x) = f\left(\widetilde{E}_s(u(g_1(\mu(x))))\right). \tag{3.19}$$

Next we study five kinds of standard pairs over $\mathbb{Q}$.

First consider the case when $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ of the first kind. If $f_1(x) = x^t$, then $t = 2$ and hence $r = 1$. Then $f_1(x) = x^2$ and $g_1(x) = axq(x)^2$ for some $q(x) \in \mathbb{Q}[x]$. Then from (3.18) we get $u(x) = x/c^2$ and hence from (3.19) it follows that

$$g(x) = f\left(\widetilde{E}_s\left(\frac{a\mu(x)q(\mu(x))^2}{c^2}\right)\right),$$

which we can write as

$$g(x) = f\left(\widetilde{E}_s\left(\delta(x)p(x)^2\right)\right) \tag{3.20}$$

with $\delta(x) = a\mu(x)/c^2$ and $p(x) = q(\mu(x))$. Clearly $\delta(x), p(x) \in \mathbb{Q}[x]$ and $\deg \delta = 1$. Now (3.8) turns into

$$f\left(\widetilde{E}_s\left(\left(h(x) - \frac{1}{2}\right)^2\right)\right) = f\left(\widetilde{E}_s\left(\delta(y)p(y)^2\right)\right). \tag{3.21}$$

We easily find a choice of parameters such that the equation (3.21) has infinitely many positive integer solutions. For example, let $\delta(x) = x$, let $r(x)$ be a polynomial which attains positive odd integer values for every $x \in \mathbb{N}$ and let $p(x) = r(x) - 1/2$. Either $h(x) = 2x$ or $h(x) = 2x + 1$, see (3.9) and (3.10), which corresponds to solutions

$$x = \frac{(4k+3)r\left((4k+3)^2\right) - (2k+1)}{2}, \quad y = (4k+3)^2,$$

and

$$x = \frac{(4k+1)r\left((4k+1)^2\right) - (2k+1)}{2}, \quad y = (4k+3)^2,$$

of the equation (3.21) for any $k \in \mathbb{N}$, respectively. Since $\deg f_1 = 2$, when $(f_1(x), g_1(x)) = \left(ax^r q(x)^t, x^t\right)$ with $0 \leq r < t$, $(r,t) = 1$, $r + \deg q > 0$, then either $r = 0$, $t = 1$ and $\deg q = 2$ or $r = 2$, $t \geq 3$ odd and $q(x)$ is a constant polynomial. In the former case we have $g_1(x) = x$ and hence from (3.19) we get

$$g(x) = f\left(\widetilde{E}_s(u(g_1(\mu(x))))\right) = f\left(\widetilde{E}_s\left(\delta(x)p(x)^2\right)\right)$$

where $p(x) = 1$ and $\delta(x) \in \mathbb{Q}[x]$ is a linear polynomial, which is a decomposition of g that already appeared, see (3.20). In the latter case we have $f_1(x) = bx^2$ and from (3.18) we get $u(x) = x/(bc^2)$, where $b \in \mathbb{Q} \setminus \{0\}$. Then

$$g(x) = f\left(\widetilde{E}_s\left(\frac{(\mu(x))^t}{bc^2}\right)\right),$$

which we can write as

$$g(x) = f\left(\widetilde{E}_s\left(\gamma\delta(x)^t\right)\right), \tag{3.22}$$

where $\gamma = 1/(bc^2)$, $\delta(x) = \mu(x)$. So, $\gamma \in \mathbb{Q}$, $\delta(x)$ is a linear polynomial in $\mathbb{Q}[x]$ and t is odd. Now (3.8) turns into

$$f\left(\widetilde{E}_s\left(\left(h(x) - \frac{1}{2}\right)^2\right)\right) = f\left(\widetilde{E}_s\left(\gamma\delta(y)^t\right)\right). \tag{3.23}$$

We easily find a choice of parameters such that the equation (3.23) has infinitely many integer solutions. For example, let $\gamma = 1/4$, $\delta(x) = x$ and $t \geq 3$ odd. For $h(x) = 2x$, and $h(x) = 2x + 1$,

$$x = \frac{(4k-1)^t + 1}{4}, \quad y = (4k-1)^2$$

and

$$x = \frac{(4k+1)^t - 1}{4}, \quad y = (4k+1)^2$$

are solutions in positive integers of the equation (3.23), respectively.

Next suppose that $(f_1(x), g_1(x))$ is a standard pair of the second kind over $\mathbb{Q}$. If $f_1(x) = (ax^2 + b)q(x)^2$, then $g_1(x) = x^2$, so from (3.19) we get

$$g(x) = f\left(\widetilde{E}_s\left(u_1\mu(x)^2 + u_0\right)\right),$$

which we can re-write as

$$g(x) = f\left(\widetilde{E}_s\left(\left(a\delta(x)^2 + b\right)p(x)^2\right)\right) \tag{3.24}$$

with $a = u_1$, $b = u_0$, $\delta(x) = \mu(x)$ and $p(x) = 1$. So, $p(x), \delta(x) \in \mathbb{Q}[x]$ and $\deg\delta = 1$. If $f_1(x) = x^2$, then from (3.18) we get $u(x) = x/c^2$ and hence

$$g(x) = f\left(\widetilde{E}_s\left(\frac{\left(a\mu(x)^2 + b\right)q(\mu(x))^2}{c^2}\right)\right),$$

which we can re-write as

$$g(x) = \left(\widetilde{E}_s\left(\left(a\delta(x)^2 + b\right)p(x)^2\right)\right), \tag{3.25}$$

with $p(x) = q(\mu(x))/c$ and $\delta(x) = \mu(x)$. Clearly $p(x), \delta(x) \in \mathbb{Q}[x]$ and $\deg\delta = 1$. Then (3.8) turns into

$$f\left(\widetilde{E}_s\left(\left(h(x) - \frac{1}{2}\right)^2\right)\right) = f\left(\widetilde{E}_s\left((a\delta(y)^2 + b)p(y)^2\right)\right). \tag{3.26}$$

Let $\delta(x) = x$, let $r(x)$ be any integer valued polynomial which attains only positive values and $p(x) = 4r(x) + 1$. Let $a = 1/2$ and $b = 1/4$. Let a_n and b_n be such that

$$a_n + b_n\sqrt{2} = (3 + 2\sqrt{2})^n, \quad n \in \mathbb{N}.$$

For $h(x) = 2x$, and $h(x) = 2x + 1$,

$$x = \frac{a_{2n+1}(4r(y) + 1) + 1}{4}, \quad y = b_{2n+1}$$

and

$$x = \frac{a_{2n}(4r(y) + 1) - 1}{4}, \quad y = b_{2n},$$

are solutions of the equation (3.26), respectively. Let now $(f_1(x), g_1(x))$ in (3.13) be a standard pair of the third kind over $\mathbb{Q}$. Then

$$(f_1(x), g_1(x)) = \left(D_2\left(x, a^t\right), D_t\left(x, a^2\right)\right)$$

with odd t. Substituting $f_1(x) = D_2(x, a^t) = x^2 - 2a^t$ into (3.18), we get $u(x) = (x + 2a^t)/c^2$, so

$$g(x) = f\left(\widetilde{E}_s\left(\frac{D_t\left(\mu(x), a^2\right) + 2a^t}{c^2}\right)\right). \tag{3.27}$$

From Theorem 3.4 it follows that the polynomial $D_t(\mu(x), a^2)/c^2$ has two extrema and those are $\pm 2a^t/c^2$. Since t is odd, both extrema are of type $(1, 2, 2, \ldots, 2)$.

From (3.27) we deduce

$$g(x) = f\left(\widetilde{E}_s\left(\delta(x)p(x)^2\right)\right) \tag{3.28}$$

with $\delta(x)$, $p(x) \in \mathbb{Q}[x]$ and $\deg \delta = 1$, which is a decomposition that already appeared, see (3.20).

Let now $(f_1(x), g_1(x))$ be a standard pair of the fourth kind over $\mathbb{Q}$. Then

$$(f_1(x), g_1(x)) = (a^{-1}D_2(x,a), b^{-t/2}D_t(x,b))$$

with even t. From (3.18) we get $u(x) = (ax+2a)/c^2$, which together with (3.13) implies

$$g(x) = f(\widetilde{E}_s(u(g_1(\mu(x))))) = f\left(\widetilde{E}_s\left(\frac{ab^{-t/2}D_t(\mu(x),b)+2a}{c^2}\right)\right).$$

The extrema of $ab^{-t/2}D_t(\mu(x),b)/c^2$ are $\pm 2b^{t/2}ab^{-t/2}/c^2 = \pm 2a/c^2$, and the extremum $-2a/c^2$ is of type $(2,2,\ldots,2)$ by Theorem 3.4. Therefore

$$g(x) = f\left(\widetilde{E}_s\left(p(x)^2\right)\right) \tag{3.29}$$

with $p(x) \in \mathbb{Q}[x]$. Then the equation (3.8) turns into

$$f\left(\widetilde{E}_s\left(\left(h(x)-\frac{1}{2}\right)^2\right)\right) = f\left(\widetilde{E}_s\left(p(y)^2\right)\right). \tag{3.30}$$

If we let $r(x)$ be an integer valued polynomial which attains only positive values and $p(x) = 2r(x) - 1/2$ if $h(x) = 2x$ and $p(x) = 2r(x) + 1/2$ if $h(x) = 2x+1$, then $(x,y) = (r(k),k)$ are solutions of the equation (3.30) for any $k \in \mathbb{N}$.

Since $\deg f_1 = 2$, the pair $(f_1(x), g_1(x))$ can not be a standard pair over $\mathbb{Q}$ of the fifth kind. □

Chapter 4

On equal values of power sums of arithmetic progressions

This chapter contains the paper [**5**] with the title *On equal values of power sums of arithmetic progressions*. It is a joint paper with András Bazsó, Florian Luca and Ákos Pintér. The article was published in *Glasnik Matematički* in 2012. The presentation of the paper here is slightly modified from the published version of the paper.

Abstract. In this paper we consider the Diophantine equation

$$b^k + (a+b)^k + \cdots + (a(x-1)+b)^k = \\ = d^l + (c+d)^l + \cdots + (c(y-1)+d)^l,$$

where a, b, c, d, k, l are given integers. We prove that, under some reasonable assumptions, this equation has only finitely many integer solutions.

1. Introduction and the main result

For integers a and b with $\gcd(a,b) = 1$ and $k, n \in \mathbb{N}$, $n \geq 2$, let

$$S_{a,b}^k(n) = b^k + (a+b)^k + \cdots + (a(n-1)+b)^k. \tag{1.1}$$

It is easy to see that the above power sum is related to the Bernoulli polynomial $B_k(x)$ in the following way:

$$S_{a,b}^k(n) = \frac{a^k}{k+1}\left(\left(B_{k+1}\left(n+\frac{b}{a}\right) - B_{k+1}\right) \right. \\ \left. - \left(B_{k+1}\left(\frac{b}{a}\right) - B_{k+1}\right)\right),$$

see [**6**] for more details. Bernoulli polynomials $B_k(x)$ are defined by the generating series

$$\frac{t\exp(tx)}{\exp(t)-1}=\sum_{k=0}^{\infty}B_k(x)\frac{t^k}{k!}.$$

For the properties of Bernoulli polynomials which will be often used in this paper, sometimes without particular reference, we refer to [**79**, Chap. 1 and 2]. We can extend the definition of $S_{a,b}^k(x)$ for every real value x as follows

$$S_{a,b}^k(x):=\frac{a^k}{k+1}\left(B_{k+1}\left(x+\frac{b}{a}\right)-B_{k+1}\left(\frac{b}{a}\right)\right). \tag{1.2}$$

As usual, we denote with $\mathbb{C}[x]$ the ring of polynomials in variable x with complex coefficients. If $G_1(x), G_2(x)\in\mathbb{C}[x]$, then $F(x)=G_1(G_2(x))$ is a functional composition of G_1 and G_2 and (G_1,G_2) is a (functional) *decomposition* of F (over $\mathbb{C}$). It is said to be nontrivial if $\deg G_1>1$ and $\deg G_2>1$. Two decompositions $F(x)=G_1(G_2(x))$ and $F(x)=H_1(H_2(x))$ are said to be *equivalent* if there exists a linear polynomial $\ell(x)\in\mathbb{C}[x]$ such that $G_1(x)=H_1(\ell(x))$ and $H_2(x)=\ell(G_2(x))$. The polynomial $F(x)$ is called *decomposable* if it has at least one nontrivial decomposition; otherwise it is said to be *indecomposable*.

In a recent paper, Bazsó, Pintér and Srivastava [**6**] proved the following theorem about decompositions of the polynomial $S_{a,b}^k(x)$.

THEOREM 1.3. *The polynomial $S_{a,b}^k(x)$ is indecomposable for even k. If $k=2v-1$ is odd, then any nontrivial decomposition of $S_{a,b}^k(x)$ is equivalent to the decomposition*

$$S_{a,b}^k(x)=\widehat{S}_v\left(\left(x+\frac{b}{a}-\frac{1}{2}\right)^2\right), \tag{1.4}$$

where $\widehat{S}_v$ is an indecomposable polynomial of degree v, which is uniquely determined by (1.4).

Using Theorem 1.3 and the general finiteness criterion of Bilu and Tichy [**13**] for Diophantine equations of the form $f(x)=g(y)$, we prove the following result.

THEOREM 1.5. *For $2\le k<l$, the equation*

$$S_{a,b}^k(x)=S_{c,d}^l(y) \tag{1.6}$$

has only finitely many solutions in integers x and y.

Since the finiteness criterion from [**13**] is based on the ineffective theorem of Siegel [**90**], Theorem 1.5 is ineffective as well. We note that for $a=c=1$, $b=d=0$ our theorem gives the result of Bilu, Brindza, Kirschenhofer, Pintér and Tichy [**12**].

Combining the result of Brindza [**16**] with recent theorems of Rakaczki [**82**] and Pintér and Rakaczki [**78**], for $k = 1$ and $k = 3$ we obtain effective results.

THEOREM 1.7. *If $l \notin \{1, 3, 5\}$, then integer solutions x, y of the equation*

$$S_{a,b}^1(x) = S_{c,d}^l(y) \tag{1.8}$$

satisfy $\max\{|x|, |y|\} < C_1$, where C_1 is an effectively computable constant depending only on a, b, c, d and l.

In the excepted cases $l = 3$ and $l = 5$ of Theorem 1.7, it is possible to find integers a, b, c, d such that the corresponding equations have infinitely many solutions. For example, if $a = 2, b = 1$, $c = 1, d = 0$ and $l = 3$, the equation (1.8) turns into

$$x^2 = 1 + 3 + \cdots + 2x - 1 = 1^3 + 2^3 + \cdots + (y-1)^3$$

and if $l = 5$, it turns into

$$x^2 = 1 + 3 + \cdots + 2x - 1 = 1^5 + 2^5 + \cdots + (y-1)^5.$$

These equations have infinitely many integer solutions, see [**87**].

THEOREM 1.9. *If $l \notin \{1, 3, 5\}$, then integer solutions x, y of the equation*

$$S_{a,b}^3(x) = S_{c,d}^l(y) \tag{1.10}$$

satisfy $\max\{|x|, |y|\} < C_2$, where C_2 is an effectively computable constant depending only on a, b, c, d and l.

2. Auxiliary results

In this section we collect some results needed to prove Theorem 1.5. First, we recall the finiteness criterion of Bilu and Tichy [**13**].

We say that the equation $f(x) = g(y)$ has infinitely many *rational solutions with a bounded denominator* if there exists $\lambda \in \mathbb{N}$ such that $f(x) = g(y)$ has infinitely many solutions $x, y \in \mathbb{Q}$ that satisfy $\lambda x, \lambda y \in \mathbb{Z}$. If the equation $f(x) = g(y)$ has only finitely many rational solutions with a bounded denominator, then it clearly has only finitely many integer solutions.

We further need to define five kinds of so-called *standard pairs* of polynomials.

In what follows a and b are nonzero rational numbers, m and n are positive integers, $r \geq 0$ is an integer and $p(x) \in \mathbb{Q}[x]$ is a nonzero polynomial (which may be constant).

A *standard pair over $\mathbb{Q}$ of the first kind* is $(x^m, ax^r p(x)^m)$, or switched, i.e $(ax^r p(x)^m, x^m)$, where $0 \leq r < m$, $\gcd(r, m) = 1$ and $r + \deg p > 0$.

A *standard pair over $\mathbb{Q}$ of the second kind* is $\left(x^2, \left(ax^2 + b\right) p(x)^2\right)$, or switched.

Denote by $D_m(x,a)$ the m-th Dickson polynomial with parameter a, defined by the functional equation

$$D_m\left(z+\frac{a}{x},a\right)=x^m+\left(\frac{a}{x}\right)^m$$

or by the explicit formula

$$D_m(x,a)=\sum_{i=0}^{\lfloor m/2\rfloor}\frac{m}{m-i}\binom{m-i}{i}(-a)^i x^{m-2i}. \tag{2.1}$$

A *standard pair over* $\mathbb{Q}$ *of the third kind* is $(D_m(x,a^n),D_n(x,a^m))$, where $\gcd(m,n)=1$.

A *standard pair over* $\mathbb{Q}$ *of the fourth kind* is

$$\left(a^{-m/2}D_m(x,a),-b^{-n/2}D_n(x,b)\right),$$

where $\gcd(m,n)=2$.

A *standard pair over* $\mathbb{Q}$ *of the fifth kind* is $\left(\left(ax^2-1\right)^3,3x^4-4x^3\right)$, or switched.

The following theorem is the main result of [**13**].

THEOREM 2.2. *Let $f(x)$ and $g(x)$ be non-constant polynomials in $\mathbb{Q}[x]$. Then the following assertions are equivalent.*

- *The equation $f(x)=g(y)$ has infinitely many rational solutions with a bounded denominator;*
- *We have*

$$f(x)=\phi(f_1(\lambda(x))),\quad g(x)=\phi(g_1(\mu(x))),$$

where $\lambda(x)$ and $\mu(x)$ are linear polynomials in $\mathbb{Q}[x]$, $\phi(x)\in\mathbb{Q}[x]$, and $(f_1(x),g_1(x))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x)=g_1(y)$ has infinitely many rational solutions with a bounded denominator.

The following lemmas are the main ingredients of the proofs of Theorems 1.7 and 1.9

LEMMA 2.3. *For every $b\in\mathbb{Q}$ and every integer $k\geq 3$ with $k\notin\{4,6\}$, the polynomial $B_k(x)+b$ has at least three zeros of odd multiplicities.*

PROOF. For $b=0$ and odd values of $k\geq 3$ this result is a consequence of the theorem of Brillhart [**15**, Corollary of Theorem 6]. For a non-zero $b\in\mathbb{Q}$ and odd k with $k\geq 3$ and for even values of $k\geq 8$, the result follows from the main theorem of [**78**] and from [**82**, Theorem 2.3], respectively. □

Our next auxiliary result is an easy consequence of an effective theorem concerning the S-integer solutions of hyperelliptic equations, which is the main result of [**16**].

LEMMA 2.4. *Let $f(x)$ be a polynomial with rational coefficients and with at least three zeros of odd multiplicities. Let u be a fixed positive integer. If x and y are integer solutions of the equation*

$$f\left(\frac{x}{u}\right) = y^2,$$

then we have $\max\{|x|, |y|\} < C_3$, *where C_3 is an effectively computable constant depending only on u and f.*

In the sequel we assume $c_1, e_1 \in \mathbb{Q} \setminus \{0\}$ and $c_0, e_0 \in \mathbb{Q}$.

LEMMA 2.5. *The polynomial $S_{a,b}^k(c_1x + c_0)$ is not of the form $e_1x^q + e_0$ with $q \geq 3$.*

LEMMA 2.6. *The polynomial $S_{a,b}^k(c_1x + c_0)$ is not of the form*

$$e_1D_m(x, \delta) + e_0,$$

where $D_m(x, \delta)$ is the m-th Dickson polynomial with $m > 4$ and $\delta \in \mathbb{Q} \setminus \{0\}$.

Before proving the lemmas above, we introduce the following notation. Let

$$S_{a,b}^k(c_1x + c_0) = s_{k+1}x^{k+1} + s_kx^k + \cdots + s_0, \tag{2.7}$$

and $c_0' := b/a + c_0$. From (1.2) we get

$$s_{k+1} = \frac{a^kc_1^{k+1}}{k+1}, \quad s_k = \frac{a^kc_1^k}{2}(2c_0' - 1) \tag{2.8}$$

$$s_{k-1} = \frac{a^kc_1^{k-1}}{12}k(6c_0'^2 - 6c_0' + 1), \ k \geq 2, \tag{2.9}$$

and for $k \geq 4$,

$$s_{k-3} = \frac{a^kc_1^{k-3}}{720}k(k-1)(k-2)(30c_0'^4 - 60c_0'^3 + 30c_0'^2 - 1). \tag{2.10}$$

PROOF OF LEMMA 2.5. Suppose that $S_{a,b}^k(c_1x + c_0) = e_1x^q + e_0$, where $q = k+1 \geq 3$. Then $s_{k-1} = 0$ and from (2.9) we get $6c_0'^2 - 6c_0' + 1 = 0$, contradiction with $c_0' \in \mathbb{Q}$. □

PROOF OF LEMMA 2.6. Suppose that $S_{a,b}^k(c_1x + c_0) = e_1D_m(x, \delta) + e_0$ with $k + 1 = m > 4$. Then

$$s_{k+1} = e_1, \quad s_k = 0, \tag{2.11}$$

$$s_{k-1} = -e_1m\delta, \tag{2.12}$$

$$s_{k-3} = \frac{e_1(m-3)m\delta^2}{2}. \tag{2.13}$$

From (2.8) and (2.11) it follows that

$$e_1 = \frac{a^{m-1}c_1^m}{m} \ \text{ and } \ c_0' = \frac{1}{2}. \tag{2.14}$$

In view of (2.9), by substituting (2.14) into (2.12), we obtain

$$c_1^2 = \frac{m-1}{24\delta}. \tag{2.15}$$

Similarly, by comparing the forms (2.10) and (2.13) of s_{k-3} and by using (2.14), we obtain

$$c_1^4 = \frac{7(m-1)(m-2)}{2880\,\delta^2}. \tag{2.16}$$

After substituting (2.15) into (2.16), we obtain $7(m-2) = 5(m-1)$, wherefrom $m = 9/2$, a contradiction. □

One can see that the condition $m > 4$ in Lemma 2.6 is necessary. Indeed,

$$S_{2,1}^2(x) = \frac{4}{3}x^3 - \frac{1}{3}x = \frac{4}{3}D_3\left(x, \frac{1}{12}\right),$$
$$S_{2,1}^3(x) = 2x^4 - x^2 = 2D_4\left(x, \frac{1}{8}\right) - \frac{1}{16}.$$

3. Proofs of the theorems

Proof of Theorem 1.7. One can rewrite the equation (1.8) as

$$\frac{c^l}{l+1}\left(B_{l+1}\left(y + \frac{d}{c}\right) - B_{l+1}\left(\frac{d}{c}\right)\right) = \frac{1}{2}ax^2 + \left(b - \frac{a}{2}\right)x,$$

that is

$$\frac{8ac^l}{l+1}\left(B_{l+1}\left(y + \frac{d}{c}\right) - B_{l+1}\left(\frac{d}{c}\right)\right) = (2ax + 2b - a)^2 - (2b - a)^2.$$

Then the result follows from Lemma 2.3 and Lemma 2.4. □

Proof of Theorem 1.9. Using (1.4) we easily see that

$$\begin{aligned} S_{a,b}^3(x) &= \frac{a^3}{4}\left(x + \frac{b}{a} - \frac{1}{2}\right)^4 - \frac{a^3}{8}\left(x + \frac{b}{a} - \frac{1}{2}\right)^2 \\ &+ \frac{a^4 - 16a^2b^2 + 32ab^3 - 16b^4}{64a}. \end{aligned}$$

Using the above representation, we rewrite the equation (1.10) as

$$64aS_{c,d}^l(y) + 3a^4 + 16a^2b^2 - 32ab^3 - 16b^4 = (X - 2a^2)^2,$$

where $X = (2ax + 2b - a)^2$. Then Lemma 2.3 and Lemma 2.4 complete the proof. □

Proof of Theorem 1.5. If the equation (1.6) has infinitely many integer solutions, then by Theorem 2.2 it follows that

$$S_{a,b}^k(a_1x + a_0) = \phi(f(x)), \quad S_{c,d}^l(b_1x + b_0) = \phi(g(x)),$$

where $(f(x), g(x))$ is a standard pair over $\mathbb{Q}$, a_0, a_1, b_0, b_1 are rationals with $a_1 b_1 \neq 0$ and $\phi(x)$ is a polynomial with rational coefficients. Assume that $h := \deg \phi > 1$. Then Theorem 1.3 implies $0 < \deg f, \deg g \leq 2$, and since $k < l$ by assumption, we have $\deg f = 1$, $\deg g = 2$. Hence $k + 1 = h$ and $l + 1 = 2h$, wherefrom $l = 2k + 1$. Since $k \geq 2$ and $l = 2k + 1$, it follows that $l \geq 5$. Since $\deg f = 1$, there exist $f_1, f_0 \in \mathbb{Q}$, $f_1 \neq 0$, such that $S^k_{a,b}(f_1 x + f_0) = \phi(x)$, so

$$S^k_{a,b}(f_1 g(x) + f_0) = \phi(g(x)) = S^l_{c,d}(b_1 x + b_0) = S^{2k+1}_{c,d}(b_1 x + b_0).$$

Since $g(x)$ is quadratic, by making the substitution $x \mapsto (x - b_0)/b_1$, we obtain that there exist $c_2, c_1, c_0 \in \mathbb{Q}$, $c_2 \neq 0$, such that

$$S^k_{a,b}(c_2 x^2 + c_1 x + c_0) = S^{2k+1}_{c,d}(x). \tag{3.1}$$

Since $\deg S^k_{a,b} = k+1 \geq 3$ and $c_2 \neq 0$, in (3.1) we have a nontrivial decomposition of $S^{2k+1}_{c,d}(x)$. From Theorem 1.3 it follows that there exists a linear polynomial $\ell(x) = Ax + B \in \mathbb{C}[x]$ such that

$$c_2 x^2 + c_1 x + c_0 = A\left(x + \frac{d}{c} - \frac{1}{2}\right)^2 + B.$$

Then clearly $A, B \in \mathbb{Q}$. From (3.1) we obtain

$$S^k_{a,b}\left(A\left(x + \frac{d}{c} - \frac{1}{2}\right)^2 + B\right) = S^{2k+1}_{c,d}(x),$$

wherefrom by linear substitution $x \mapsto x - d/c + 1/2$ we obtain

$$S^k_{a,b}(Ax^2 + B) = S^{2k+1}_{c,d}\left(x - \frac{d}{c} + \frac{1}{2}\right). \tag{3.2}$$

Thus, we have an equality of polynomials of degrees $2k + 2 \geq 6$. We calculate and compare coefficients of the first few highest monomials of the polynomials in (3.2). The coefficients of the polynomial on the right-hand side are easily deduced by setting $c_1 = 1, c_0 = -d/c + 1/2$ into (2.8), (2.9) and (2.10). Therefrom it follows that if we denote

$$S^{2k+1}_{c,d}\left(x - \frac{d}{c} + \frac{1}{2}\right) = r_{2k+2}x^{2k+2} + \cdots + r_1 x + r_0,$$

then we get

$$\begin{aligned} r_{2k+2} &= \frac{c^{2k+1}}{2k+2}, \quad r_{2k+1} = 0, \\ r_{2k} &= \frac{-c^{2k+1}(2k+1)}{24}, \\ r_{2k-2} &= \frac{7c^{2k+1}(2k+1)k(2k-1)}{2880}. \end{aligned}$$

The coefficients $s_{k+1}, s_k, s_{k-1}, s_{k-3}$ of the polynomial $S_{a,b}^k(x)$ can be found by setting $c_1 = 1, c_0 = 0$ into equations (2.8), (2.9) and (2.10). Since

$$S_{a,b}^k(Ax^2 + B) = \sum_{m=0}^{k+1} s_m \sum_{i=0}^{m} \binom{m}{i} \left(Ax^2\right)^i B^{m-i},$$

it follows that if we denote

$$S_{a,b}^k(Ax^2 + B) = t_{2k+2}x^{2k+2} + \cdots + t_1 x + t_0,$$

then

$$\begin{aligned} t_{2k+2} &= \frac{a^k A^{k+1}}{k+1}, \quad t_{2k+1} = 0, \\ t_{2k} &= a^k A^k B + \frac{a^k A^k}{2}\left(2\left(\frac{b}{a}\right) - 1\right), \\ t_{2k-2} &= \frac{a^k k}{2} A^{k-1} B^2 + \frac{a^k k}{2} A^{k-1} B \left(2\left(\frac{b}{a}\right) - 1\right) \\ &+ \frac{a^k k}{12} A^{k-1}\left(6\left(\frac{b}{a}\right)^2 - 6\left(\frac{b}{a}\right) + 1\right). \end{aligned}$$

Next we compare coefficients. It must be $r_i = t_i$ for all $i = 0, 1, \ldots, 2k+2$. Comparing the leading coefficients yields

$$\frac{a^k A^{k+1}}{k+1} = \frac{c^{2k+1}}{2k+2}, \qquad \text{so} \qquad 2a^k A^{k+1} = c^{2k+1}. \tag{3.3}$$

By comparing the coefficients of index $2k$ and using (3.3) we obtain

$$\frac{b}{a} - \frac{1}{2} = -\frac{1}{12}A(2k+1) - B. \tag{3.4}$$

By comparing the coefficients of index $2k-2$ and after simplifying we obtain

$$\frac{B^2}{2} + \frac{B}{2}\left(2\left(\frac{b}{a}\right) - 1\right) + \frac{1}{12}\left(6\left(\frac{b}{a}\right)^2 - 6\left(\frac{b}{a}\right) + 1\right) = \frac{7(4k^2-1)A^2}{1440}.$$

From (3.4) it follows that the last relation above can be transformed into

$$\begin{aligned} \frac{B^2}{2} + B\left(-\frac{1}{12}A(2k+1) - B\right) &+ \frac{1}{2}\left(-\frac{1}{12}A(2k+1) - B\right)^2 - \frac{1}{24} \\ &= \frac{7A^2(4k^2-1)}{1440}. \end{aligned}$$

After simplification we obtain

$$A^2(k-3)(-2k-1) = 15.$$

For $k \geq 3$, the expression on the left-hand side above is negative or zero, contradiction. If $k = 2$, then $A^2 = 3$, which contradicts $A \in \mathbb{Q}$. Therefore, there are

no rational coefficients a, b, c, d, A and B such that (3.2) is satisfied, wherefrom it follows that $\deg \phi = 1$.

If $\deg \phi = 1$, then we have

$$S^k_{a,b}(a_1x + a_0) = e_1 f(x) + e_0, \qquad S^l_{c,d}(b_1x + b_0) = e_1 g(x) + e_0,$$

where $e_1, e_0 \in \mathbb{Q}$, $e_1 \neq 0$. Clearly $\deg f = k + 1$ and $\deg g = l + 1$.

In view of the assumptions on k and l, it follows that $(f(x), g(x))$ cannot be a standard pair over $\mathbb{Q}$ of the second kind, and with the exception of the case $(k, l) = (3, 5)$, of the fifth kind either. If $(k, l) = (3, 5)$, by using formula (2.9) for $k = 3$, it is easy to see that $S^3_{a,b}(c_1x + c_0) = e_1(3x^4 - 4x^3) + e_0$ is not possible.

If $(f(x), g(x))$ is of the first kind, then one of the polynomials $S^k_{a,b}(a_1x + a_0)$ and $S^l_{c,d}(b_1x + b_0)$ is of the form $e_1x^q + e_0$ with $q \geq 3$. This is impossible by Lemma 2.5.

If $(f(x), g(x))$ is a standard pair of the third or fourth kind, then we have that either $S^l_{c,d}(b_1x + b_0) = e_1 D_m(x, \delta) + e_0$ with $m = l + 1 \geq 5$ and $\delta \in \mathbb{Q} \setminus \{0\}$, which contradicts Lemma 2.6, or $k = 2, l = 3$. In the latter case, Theorem 1.9 gives an effective finiteness statement. □

Chapter 5

Non-extensibility of the pair $\{1,3\}$ to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{-d}\right]$

This chapter contains the paper [**40**] with the title *Non-extensibility of the pair* $\{1,3\}$ *to a Diophantine quintuple in* $\mathbb{Z}\left[\sqrt{-d}\right]$. It is a joint paper with Zrinka Franušić. The article was published in *Journal of Combinatorics and Number Theory* in 2011. The presentation of the paper here is slightly modified from the published version of the paper.

Abstract. We show that the Diophantine pair $\{1,3\}$ can not be extended to a Diophantine quintuple in the ring $\mathbb{Z}\left[\sqrt{-2}\right]$. This result completes the work of the first author and establishes non-extensibility of the Diophantine pair $\{1,3\}$ to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{-d}\right]$ for all $d \in \mathbb{N}$.

1. Introduction and results

Let R be a commutative ring with unity 1. The set $\{a_1, a_2, \ldots, a_m\}$ in R such that $a_i \neq 0$ for all $i = 1, \ldots, m$, $a_i \neq a_j$ and $a_i a_j + 1$ is a square in R for all $1 \leq i < j \leq m$, is called a *Diophantine m-tuple* in R. The problem of constructing such sets was first studied by Diophantus of Alexandria who found a set of four rationals $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$ with the given property. Fermat found a first Diophantine quadruple in integers - the set $\{1, 3, 8, 120\}$. A Diophantine pair $\{a, b\}$ in a ring R, which satisfies $ab + 1 = r^2$, can be extended to a Diophantine quadruple in R by adding elements $a + b + 2r$ and $4r(r + a)(r + b)$, provided all four elements are nonzero and different. Hence, apart from some exceptional cases, Diophantine quadruples in a ring R exist, but can we obtain Diophantine m-tuples of size greater than 4?

The folklore conjecture is that there are no Diophantine quintuples in integers. In 1969, Baker and Davenport [**3**] showed that the set $\{1,3,8\}$ can not be extended to a Diophantine quintuple, which was the first result supporting the conjecture. This result was first generalized by Dujella [**27**], who showed that the set $\{k-1,k+1,4k\}$, with integer $k\geq 2$, can not be extended to a Diophantine quintuple in $\mathbb{Z}$. Dujella and Pethő [**33**] later showed that not even the Diophantine pair $\{1,3\}$ can be extended to a Diophantine quintuple in $\mathbb{Z}$. Greatest step towards proving the conjecture did Dujella [**29**] in 2004; he showed that there are no Diophantine sextuples in integers and that there are only finitely many Diophantine quintuples. In [**30**] it was proved that there are no Diophantine quintuples in the ring of polynomials with integers coefficients under assumption that not all elements are constant polynomials.

The size of Diophantine m-tuples can be greater than 4 in some rings. For instance, the set

$$\left\{\frac{11}{192},\frac{35}{192},\frac{155}{27},\frac{512}{27},\frac{1235}{48},\frac{180873}{16}\right\}$$

is a Diophantine sextuple in $\mathbb{Q}$; it was found by Gibbs [**49**].

Furthermore, we can construct Diophantine quintuples in the ring $\mathbb{Z}\left[\sqrt{d}\right]$ for some values of d; for instance $\{1,3,8,120,1678\}$ is a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{201361}\right]$. It is natural to start investigating the upper bound for the size of Diophantine m-tuples in $\mathbb{Z}\left[\sqrt{d}\right]$ by focusing on a problem of extensibility of Diophantine triples $\{k-1,k+1,4k\}$ and Diophantine pair $\{1,3\}$ to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{d}\right]$, since the problem in integers was approached similarly, see [**33**] and [**27**]. In [**39**] Franušić proved that the Diophantine pair $\{1,3\}$ can not be extended to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{-d}\right]$ if d is a positive integer and $d\neq 2$. The case $d=2$ was also considered and it was shown that if $\{1,3,c\}$ is a Diophantine triple in $\mathbb{Z}\left[\sqrt{-2}\right]$, then $c\in\{c_k,d_l\}$, where the sequences (c_k) and (d_l) are given by

$$c_k=\frac{1}{6}\big((2+\sqrt{3})(7+4\sqrt{3})^k+(2-\sqrt{3})(7-4\sqrt{3})^k-4\big), \tag{1.1}$$

$$d_l=\frac{-1}{6}\big((7+4\sqrt{3})^l+(7-4\sqrt{3})^l+4\big), \tag{1.2}$$

where $k\geq 1$ and $l\geq 0$. Sequences (c_k) and (d_l) are defined recursively as follows

$$c_0=0, \qquad c_1=8, \qquad c_{k+2}=14c_{k+1}-c_k+6; \tag{1.3}$$

$$d_0=-1, \qquad d_1=-3, \qquad d_{l+2}=14d_{l+1}-d_l+8. \tag{1.4}$$

It is known that $\{1,3,c_k,c_{k+1}\}$, with $k\geq 1$, is a Diophantine quadruple in integers, see [**33**], and is hence also in $\mathbb{Z}\left[\sqrt{-2}\right]$. The set $\{1,3,d_l,d_{l+1}\}$ is a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$ since

$$d_ld_{l+1}+1=(c_l+2)^2 \tag{1.5}$$

for every $l \geq 0$; this easily follows from identities (1.1) and (1.2). The set $\{1, 3, c_k, d_l\}$ is not a Diophantine quadruple for $k \geq 1$ and $l \geq 0$ since $1 + c_k d_l$ is a negative odd number and hence it can not be a square in $\mathbb{Z}\left[\sqrt{-2}\right]$. Therefore, if there is an extension of the Diophantine pair $\{1, 3\}$ to a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$, then it is of the form $\{1, 3, c_k, c_l\}$, with $l > k \geq 1$ or $\{1, 3, d_k, d_l\}$, with $l > k \geq 0$. In the former case, the set can not be extended to a Diophantine quintuple in $\mathbb{Z}$, see [**33**], wherefrom it easily follows that it can not be extended to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{-2}\right]$. It remains to examine the latter case. We can formulate the following theorem.

THEOREM 1.6. *Let k be a nonnegative integer and d an integer. If the set $\{1, 3, d_k, d\}$ is a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$, where d_k is given by* (1.2), *then $d = d_{k-1}$ or $d = d_{k+1}$.*

From Theorem 1.6 we immediately obtain the following corollary.

COROLLARY 1.7. *The Diophantine pair $\{1, 3\}$ can not be extended to a Diophantine quintuple in $\mathbb{Z}\left[\sqrt{-2}\right]$.*

The organization of the paper is as follows. In Section 2, assuming k to be minimal integer for which Theorem 1.6 does not hold, we translate the assumption of Theorem 1.6 into system of Pellian equations from which recurrent sequences $\nu_m^{(i)}$ and $\omega_n^{(j)}$ are deduced, intersections of which give solutions to the system. In Section 3 we use a congruence method introduced by Dujella and Pethő [**33**] to determine the fundamental solutions of Pellian equations. In Section 4 we give a lower bound for m and n for which the sequences $\nu_m^{(i)}$ and $\omega_n^{(j)}$ intersect. In Section 5 we use a theorem of Bennett [**9**] to establish an upper bound for k. Remaining cases are examined separately in Section 6 using linear forms in logarithms, Baker-Wüstholz theorem [**4**] and the Baker-Davenport method of reduction [**3**].

2. The system of Pellian equations

Let $\{1, 3, d_k, d\}$ be a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$ where k is the minimal integer for which Theorem 1.6 does not hold. Assume $k \geq 6$. Clearly $d = d_l$ for some $l \geq 0$. Since $d + 1$ and $3d + 1$ are negative integers and $d_k d + 1$ is a positive integer, it follows that there exist $x, y, z \in \mathbb{Z}$ such that

$$d + 1 = -2x^2, \qquad 3d + 1 = -2y^2, \qquad d_k d + 1 = z^2. \tag{2.1}$$

The system of equations (2.1) is equivalent to the following system of Pellian equations

$$z^2 + 2d_k x^2 = 1 - d_k \tag{2.2}$$

$$3z^2 + 2d_k y^2 = 3 - d_k \tag{2.3}$$

where

$$d_k+1=-2s_k^2, \qquad 3d_k+1=-2t_k^2, \tag{2.4}$$

for some $s_k, t_k \in \mathbb{Z}$. Note that we may assume $s_k, t_k \in \mathbb{N}$. Conditions (2.4) follow from the fact that $\{1,3,d_k\}$ is a Diophantine triple in $\mathbb{Z}\left[\sqrt{-2}\right]$ and the fact that d_k+1 and $3d_k+1$ are negative integers.

The following propositions describe the set of positive integer solutions of equations (2.2) and (2.3).

PROPOSITION 2.5. *There exist $i_0 \in \mathbb{N}$ and $z_0^{(i)}, x_0^{(i)} \in \mathbb{Z}$, $i=1,2,\ldots,i_0$, such that $\left(z_0^{(i)}, x_0^{(i)}\right)$ are solutions of the equation* (2.2)*, which satisfy*

$$1 \leq z_0^{(i)} \leq \sqrt{-d_k(1-d_k)}, \qquad 1 \leq \left|x_0^{(i)}\right| \leq \sqrt{\frac{1-d_k^2}{2d_k}},$$

and such that for every solution $(z,x) \in \mathbb{N}\times\mathbb{N}$ of the equation (2.2)*, there exists $i \in \{1,2,\ldots,i_0\}$ and an integer $m \geq 0$ such that*

$$z+x\sqrt{-2d_k} = \left(z_0^{(i)}+x_0^{(i)}\sqrt{-2d_k}\right)\left(-2d_k-1+2s_k\sqrt{-2d_k}\right)^m.$$

PROOF. The fundamental solution of the related Pell's equation $z^2+2d_kx^2=1$ is $-2d_k-1+2s_k\sqrt{-2d_k}$ since

$$(-2d_k-1)^2+2d_k\cdot(2s_k)^2 = 4d_k^2+4d_k+1-4d_k(1+d_k)=1$$

and $-2d_k-1>2s_k^2-1=-d_k-2$, see [**72**, Theorem 105]. Following arguments of Nagell [**72**, Theorem 108] we obtain that there are finitely many integer solutions $\left(z_0^{(i)}, x_0^{(i)}\right)$, $i=1,2,\ldots,i_0$ of the equation (2.2) such that the following inequalities hold

$$1 \leq \left|z_0^{(i)}\right| \leq \sqrt{-d_k(1-d_k)}, \qquad 0 \leq \left|x_0^{(i)}\right| \leq \sqrt{\frac{1-d_k^2}{2d_k}},$$

and such that if $z+x\sqrt{-2d_k}$ is a solution of the equation (2.2) with z and x in $\mathbb{Z}$, then

$$z+x\sqrt{-2d_k} = \left(z_0^{(i)}+x_0^{(i)}\sqrt{-2d_k}\right)\left(-2d_k-1+2s_k\sqrt{-2d_k}\right)^m$$

for some $m \in \mathbb{Z}$ and $i \in \{1,2,\ldots,i_0\}$. Hence

$$z_0^{(i)}+x_0^{(i)}\sqrt{-2d_k} = \left(z+x\sqrt{-2d_k}\right)\left(-2d_k-1+2s_k\sqrt{-2d_k}\right)^{-m},$$

wherefrom it can be easily deduced that if $z+x\sqrt{-2d_k}$ is a solution of the equation (2.2) with z and x in $\mathbb{N}$, then $z_0^{(i)}>0$. Hence

$$1 \leq z_0^{(i)} \leq \sqrt{-d_k(1-d_k)}$$

for all $i \in \{1, 2, \ldots, i_0\}$. If $x_0^{(i)} = 0$, we get a contradiction with the upper bound for $z_0^{(i)}$, hence $\left|x_0^{(i)}\right| \geq 1$. To complete the proof it remains to show that $m \geq 0$. Assume to the contrary that $m < 0$. Then

$$\left(-2d_k - 1 + 2s_k\sqrt{-2d_k}\right)^m = \alpha - \beta\sqrt{-2d_k}$$

with $\alpha, \beta \in \mathbb{N}$ and $\alpha^2 + 2d_k\beta^2 = 1$. Since

$$z + x\sqrt{-2d_k} = \left(z_0^{(i)} + x_0^{(i)}\sqrt{-2d_k}\right)\left(\alpha - \beta\sqrt{-2d_k}\right),$$

we have $x = -z_0^{(i)}\beta + x_0^{(i)}\alpha$. By squaring $x_0^{(i)}\alpha = x + z_0^{(i)}\beta$ and substituting $\alpha^2 = 1 - 2d_k\beta^2$ we get

$$\left(x_0^{(i)}\right)^2 = \beta^2(1 - d_k) + x^2 + 2xz_0^{(i)}\beta > \beta^2(1 - d_k) \geq 1 - d_k > \frac{1 - d_k^2}{2d_k},$$

since x, $z_0^{(i)}$, β and k are positive integers. This is in contradiction with the upper bound for $x_0^{(i)}$. □

Using the same arguments we can prove the following proposition.

PROPOSITION 2.6. *There exists $j_0 \in \mathbb{N}$ and $z_1^{(j)}, y_1^{(j)} \in \mathbb{Z}$, $j = 1, 2, \ldots, j_0$, such that $\left(z_1^{(j)}, y_1^{(j)}\right)$ are solutions of the equation* (2.3)*, which satisfy*

$$1 \leq z_1^{(j)} \leq \sqrt{-d_k(3 - d_k)}, \qquad 1 \leq \left|y_1^{(j)}\right| \leq \sqrt{\frac{(3 - d_k)(1 + 3d_k)}{2d_k}},$$

and such that for every solution $(z, y) \in \mathbb{N} \times \mathbb{N}$ of the equation (2.3)*, there exists $j \in \{1, 2, \ldots, j_0\}$ and an integer $n \geq 0$ such that*

$$z\sqrt{3} + y\sqrt{-2d_k} = \left(z_1^{(j)}\sqrt{3} + y_1^{(j)}\sqrt{-2d_k}\right)\left(-6d_k - 1 + 2t_k\sqrt{-6d_k}\right)^n.$$

□

Finitely many solutions that satisfy bounds given in Proposition 2.5 and Proposition 2.6 will be called *fundamental* solutions.

From Proposition 2.5 and Proposition 2.6 it follows that if (z, x) is a solution in positive integers of the equation (2.2), then $z = \nu_m^{(i)}$ for some $m \geq 0$ and $i \in \{1, 2, \ldots, i_0\}$, where

$$\begin{aligned} \nu_0^{(i)} &= z_0^{(i)}, \\ \nu_1^{(i)} &= (-2d_k - 1)z_0^{(i)} - 4s_k d_k x_0^{(i)}, \\ \nu_{m+2}^{(i)} &= (-4d_k - 2)\nu_{m+1}^{(i)} - \nu_m^{(i)}, \end{aligned} \tag{2.7}$$

and if (z,y) is a solution in positive integers of the equation (2.3), then $z=\omega_n^{(j)}$ for some $n\geq 0$ and $j\in\{1,2,\ldots,j_0\}$, where

$$\begin{aligned}\omega_0^{(j)}&=z_1^{(j)},\\ \omega_1^{(j)}&=(-6d_k-1)z_1^{(j)}-4t_kd_ky_1^{(j)},\\ \omega_{n+2}^{(j)}&=(-12d_k-2)\omega_{n+1}^{(j)}-\omega_n^{(j)}.\end{aligned}\tag{2.8}$$

Therefore, we are looking for the intersection of sequences $\nu_m^{(i)}$ and $\omega_n^{(j)}$.

3. Congruence method

Using the congruence method introduced by Dujella and Pethő [**33**] we determine the fundamental solutions of the equations (2.2) and (2.3).

Lemma 3.1.

$$\begin{aligned}\nu_{2m}^{(i)}&\equiv z_0^{(i)} \pmod{-2d_k}, & \nu_{2m+1}^{(i)}&\equiv -z_0^{(i)} \pmod{-2d_k},\\ \omega_{2n}^{(j)}&\equiv z_1^{(j)} \pmod{-2d_k}, & \omega_{2n+1}^{(j)}&\equiv -z_1^{(j)} \pmod{-2d_k},\end{aligned}$$

for all $m,n\geq 0$, $i\in\{1,2,\ldots,i_0\}$, $j\in\{1,2,\ldots,j_0\}$.

Proof. Easily follows by induction. □

Lemma 3.2. *If* $\nu_m^{(i)}=\omega_n^{(j)}$ *for some* $m,n\geq 0$, $i\in\{1,2,\ldots,i_0\}$, $j\in\{1,2,\ldots,j_0\}$, *then* $z_0^{(i)}=z_1^{(j)}$ *or* $z_0^{(i)}+z_1^{(j)}=-2d_k$.

Proof. From Lemma 3.1 it follows that either $z_0^{(i)}\equiv z_1^{(j)} \pmod{-2d_k}$ or $z_0^{(i)}\equiv -z_1^{(j)} \pmod{-2d_k}$. In the latter case $z_0^{(i)}+z_1^{(j)}\equiv 0 \pmod{-2d_k}$. From Proposition 2.5 and Proposition 2.6 we get

$$\begin{aligned}0<z_0^{(i)}+z_1^{(j)}&\leq\sqrt{-d_k(1-d_k)}+\sqrt{-d_k(3-d_k)}\\ &<-d_k+1-d_k+2=-2d_k+3,\end{aligned}$$

wherefrom it follows that $z_0^{(i)}+z_1^{(j)}=-2d_k$. If $z_0^{(i)}\equiv z_1^{(j)} \pmod{-2d_k}$ and $z_0^{(i)}>z_1^{(j)}$, then

$$0<z_0^{(i)}-z_1^{(j)}<z_0^{(i)}\leq\sqrt{-d_k(1-d_k)}<-2d_k,$$

contradiction. Analogously, if $z_1^{(j)}>z_0^{(i)}$, then

$$0<z_1^{(j)}-z_0^{(i)}<z_1^{(j)}\leq\sqrt{-d_k(3-d_k)}<-2d_k,$$

contradiction. □

Lemma 3.3.

$$\nu_m^{(i)}\equiv(-1)^m\left(z_0^{(i)}+2d_km^2z_0^{(i)}+4d_ks_kmx_0^{(i)}\right) \pmod{8d_k^2}\tag{3.4}$$

$$\omega_n^{(j)}\equiv(-1)^n\left(z_1^{(j)}+6d_kn^2z_1^{(j)}+4d_kt_kny_1^{(j)}\right) \pmod{8d_k^2}\tag{3.5}$$

for all $m, n \geq 0$, $i \in \{1, 2, \ldots, i_0\}$, $j \in \{1, 2, \ldots, j_0\}$.

PROOF. Easily follows by induction. □

LEMMA 3.6. *If* $\nu_m^{(i)} = \omega_n^{(j)}$ *for some* $m, n \geq 0$, $i \in \{1, 2, \ldots, i_0\}$, $j \in \{1, 2, \ldots, j_0\}$, *then* $m \equiv n \pmod 2$.

PROOF. If m is even and n odd, then Lemma 3.1 and Lemma 3.2 imply $z_0^{(i)} + z_1^{(j)} = -2d_k$. Lemma 3.3 implies

$$z_0^{(i)} + 2d_k m^2 z_0^{(i)} + 4d_k s_k m x_0^{(i)} \equiv -z_1^{(j)} - 6d_k n^2 z_1^{(j)} - 4d_k t_k n y_1^{(j)} \pmod{8d_k^2},$$

wherefrom, by substituting $z_0^{(i)} + z_1^{(j)} = -2d_k$ and dividing by $2d_k$, we obtain

$$-1 + m^2 z_0^{(i)} + 2s_k m x_0^{(i)} \equiv -3n^2 z_1^{(j)} - 2t_k n y_1^{(j)} \pmod{-4d_k}.$$

Since d_k is always odd, from (2.2) and (2.3) we get that $z_0^{(i)}$ and $z_1^{(j)}$ are even, hence the last congruence can not hold. Indeed, on the left side is an odd integer and on the right side is an even integer, contradiction. If m is odd and n even, a contradiction can be obtained analogously. □

Therefore, the equations $\nu_{2m}^{(i)} = \omega_{2n+1}^{(j)}$ and $\nu_{2m+1}^{(i)} = \omega_{2n}^{(j)}$ have no solutions in integers $m, n \geq 0$, $i \in \{1, 2, \ldots, i_0\}$, $j \in \{1, 2, \ldots, j_0\}$.

It remains to examine the cases when m and n are both even or both odd. In each of those cases we have $z_0^{(i)} = z_1^{(j)}$. Since

$$\left(z_0^{(i)}\right)^2 - 1 = d_k \left(-2\left(x_0^{(i)}\right)^2 - 1\right),$$

it follows that

$$\delta := \frac{\left(z_0^{(i)}\right)^2 - 1}{d_k}$$

is an integer. Furthermore,

$$\delta + 1 = -2\left(x_0^{(i)}\right)^2, \qquad 3\delta + 1 = -2\left(y_1^{(j)}\right)^2, \qquad \delta d_k + 1 = \left(z_0^{(i)}\right)^2.$$

Thus δ satisfies system (2.1) and hence $\delta = d_l$ for some $l \geq 0$. Moreover, $\{1, 3, d_k, d_l\}$ is a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$ since $d_l \neq d_k$. Indeed, if $d_l = d_k$ then

$$d_k^2 + 1 = \left(z_0^{(i)}\right)^2,$$

contradiction with $d_k^2 \equiv 1 \pmod 4$. In what follows we show that $l = k - 1$. Assume $\delta > d_{k-1}$, that is $l < k - 1$. Then the triple $\{1, 3, d_l\}$ can be extended to a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$ by d_k, which differs from d_{l-1} and d_{l+1} since $l - 1 < l + 1 < k$ by assumption; this contradicts the minimality of k. Therefore $l \geq k - 1$. On the other hand, since

$$\delta d_k + 1 = \left(z_0^{(i)}\right)^2 \leq -d_k(-d_k + 1),$$

from Proposition 2.5 it follows that $\delta = d_l > d_k - 1$ and hence $l \leq k$. Since $d_l \neq d_k$ we have $d_l = d_{k-1}$. Hence

$$\left(z_0^{(i)}\right)^2 = d_k d_{k-1} + 1.$$

From (1.5) we obtain $z_0^{(i)} = z_0 = c_{k-1} + 2$. Furthermore, from (2.2), (2.3) and (2.4) we get $\left|x_0^{(i)}\right| = s_{k-1}$ and $\left|y_1^{(j)}\right| = t_{k-1}$. Moreover, from

$$s_k = \frac{1}{2\sqrt{3}}\left(\left(2+\sqrt{3}\right)^k - \left(2-\sqrt{3}\right)^k\right),$$
$$t_k = \frac{1}{2}\left(\left(2+\sqrt{3}\right)^k + \left(2-\sqrt{3}\right)^k\right),$$

we get

$$2s_k s_{k-1} = c_{k-1}, \qquad 2t_k t_{k-1} = 3c_{k-1} + 4. \tag{3.7}$$

This brings us to the important conclusion. If the system of Pellian equations (2.2) and (2.3) has a solution in positive integers, where k is the smallest integer for which Theorem 1.6 does not hold and under assumption $k \geq 6$, the fundamental solutions of Pellian equations (2.2) and (2.3) are $(z_0, x_0^{\pm})$ and $(z_1, y_1^{\pm})$ respectively, where

$$z_0 = z_1 = 2(s_k s_{k-1} + 1), \tag{3.8}$$

$$x_0^{\pm} = \pm s_{k-1}, \quad y_1^{\pm} = \pm t_{k-1}. \tag{3.9}$$

4. The lower bound for m and n

After plugging (3.8) and (3.9) into (2.7) and (2.8) and expanding we get

$$\nu_m^{\pm} = \frac{1}{2}\left(2(s_k s_{k-1}+1) \pm s_{k-1}\sqrt{-2d_k}\right)\left(-2d_k - 1 + 2s_k\sqrt{-2d_k}\right)^m$$
$$+ \frac{1}{2}\left(2(s_k s_{k-1}+1) \mp s_{k-1}\sqrt{-2d_k}\right)\left(-2d_k - 1 - 2s_k\sqrt{-2d_k}\right)^m,$$

and

$$\omega_n^{\pm} = \frac{1}{2\sqrt{3}}\left(2(s_k s_{k-1}+1)\sqrt{3} \pm t_{k-1}\sqrt{-2d_k}\right)\left(-6d_k - 1 + 2t_k\sqrt{-6d_k}\right)^n$$
$$+ \frac{1}{2\sqrt{3}}\left(2(s_k s_{k-1}+1)\sqrt{3} \mp t_{k-1}\sqrt{-2d_k}\right)\left(-6d_k - 1 - 2t_k\sqrt{-6d_k}\right)^n,$$

for $m, n \geq 0$. One intersection of these sequences is clearly

$$\nu_0^{\pm} = \omega_0^{\pm} = 2(s_k s_{k-1} + 1),$$

wherefrom it follows that the triple $\{1, 3, d_k\}$ can be extended to a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$ by d_{k-1}. Another intersection is $\nu_1^- = \omega_1^-$. Indeed, (3.7)

implies

$$s_k s_{k-1} + 1 = \frac{1}{3}\left(t_k t_{k-1} + 1\right) \tag{4.1}$$

and hence

$$\begin{aligned}\omega_1^- &= -2 - 12d_k - 2s_k s_{k-1} - 12d_k s_k s_{k-1} + 4d_k t_k t_{k-1} \\ &= -2 - 4d_k - 2s_k s_{k-1} = \nu_1^-.\end{aligned}$$

Therefrom it follows that the triple $\{1, 3, d_k\}$ can be extended to a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$ by d_{k+1}. Using (4.1) we can write $\omega_n^{\pm}$ as follows

$$\begin{aligned}\omega_n^{\pm} = &\frac{1}{6}\left(2(t_k t_{k-1} + 1) \pm t_{k-1}\sqrt{-6d_k}\right)\left(-6d_k - 1 + 2t_k\sqrt{-6d_k}\right)^n \\ &+ \frac{1}{6}\left(2(t_k t_{k-1} + 1) \mp t_{k-1}\sqrt{-6d_k}\right)\left(-6d_k - 1 - 2t_k\sqrt{-6d_k}\right)^n.\end{aligned}$$

Since

$$\begin{aligned}2(s_k s_{k-1} + 1) - s_{k-1}\sqrt{-2d_k} &= 2 - \frac{\sqrt{-2d_{k-1} - 2}}{\sqrt{-2d_k - 2} + \sqrt{-2d_k}} \\ &> 2 - \frac{\sqrt{-2d_k - 2}}{\sqrt{-2d_k - 2} + \sqrt{-2d_k}} > 1,\end{aligned}$$

it follows that

$$\nu_m^+ \geq \nu_m^- > \frac{1}{2}\left(-2d_k - 1 + 2s_k\sqrt{-2d_k}\right)^m.$$

Furthermore,

$$\omega_n^- \leq \omega_n^+ < \frac{1}{2}\left(-6d_k - 1 + 2t_k\sqrt{-6d_k}\right)^{n+1},$$

since

$$2(t_k t_{k-1} + 1) - t_{k-1}\sqrt{-6d_k} < \left(\frac{-6d_k - 1 - 2t_k\sqrt{-6d_k}}{-6d_k - 1 + 2t_k\sqrt{-6d_k}}\right)^n$$

and

$$\frac{1}{3}\left(2(t_k t_{k-1} + 1) + t_{k-1}\sqrt{-6d_k} + 1\right) < -6d_k - 1 + 2t_k\sqrt{-6d_k},$$

which can be easily verified using (2.4). Therefore, if one of the equations $\nu_m^{\pm} = \omega_n^{\pm}$ has solutions, then

$$\frac{1}{2}\left(-2d_k - 1 + 2s_k\sqrt{-2d_k}\right)^m < \frac{1}{2}\left(-6d_k - 1 + 2t_k\sqrt{-6d_k}\right)^{n+1},$$

wherefrom

$$\frac{m}{n+1} < \frac{\log\left(-6d_k - 1 + 2t_k\sqrt{-6d_k}\right)}{\log\left(-2d_k - 1 + 2s_k\sqrt{-2d_k}\right)}.$$

The expression on the right side of the inequality decreases when k increases. Since $k \geq 6$ it follows that

$$\frac{m}{n+1} < 1.072.$$

We may assume $n \geq 2$. Indeed for $n = 1$ we have $m \leq 2$ and since m and n are both even or both odd it follows that the only possibility is $m = 1$. We have already established the intersection $\nu_1^- = \omega_1^-$ and it can be easily verified that $\nu_1^+ \neq \omega_1^\pm$ and $\nu_1^- \neq \omega_1^+$. Now it can be easily deduced that $m < n\sqrt{3}$. Hence, if the sequences $(\nu_m^\pm)$ and $(\omega_n^\pm)$ have any intersections besides two already established ones, then $n \geq 2$, m and n are of the same parity and $m < n\sqrt{3}$. We further on assume these conditions.

PROPOSITION 4.2. *Let $n \geq 2$. If one of the equations $\nu_m^\pm = \omega_n^\pm$ has solutions then*

$$m \geq n \geq \frac{2}{3} \cdot \sqrt[4]{-d_k}.$$

PROOF. If $m < n$, then $m \leq n - 2$, since m and n are of the same parity. From (2.7) and (2.8) using (3.7) one easily finds $\nu_0^+ < \omega_2^-$. It can be shown by induction that $\nu_m^+ < \omega_{m+2}^-$ for $m \geq 0$. Indeed, sequences $(\nu_m^\pm)$ and $(\omega_n^\pm)$ are strictly increasing positive sequences, which can be easily checked by induction after plugging (3.8) and (3.9) into (2.7) and (2.8). Hence

$$\nu_{m+1}^+ < (-4d_k - 2)\nu_m^+, \qquad \omega_{m+3}^- > (-12d_k - 3)\omega_{m+2}^-.$$

Then clearly $\nu_m^+ < \omega_{m+2}^-$ implies $\nu_{m+1}^+ < \omega_{m+3}^-$, which completes the proof by induction. Since

$$\nu_m^- \leq \nu_m^+ < \omega_{m+2}^- \leq \omega_{m+2}^+,$$

it follows that if one of the equations $\nu_m^\pm = \omega_n^\pm$ has solutions, then $m + 2 > n$, a contradiction. Hence $m \geq n$. For the second part of the statement assume to the contrary that $n < \frac{2}{3}\sqrt[4]{-d_k}$. Let us show how we can reach a contradiction in the case $\nu_m^+ = \omega_n^+$. Other three case can be similarly resolved. Since m and n are of the same parity, Lemma 3.3 implies that if $\nu_m^+ = \omega_n^+$, then

$$(c_{k-1} + 2)(m^2 - 3n^2 + m - 3n) \equiv 2(m - n) \pmod{-4d_k}, \tag{4.3}$$

and since (1.5) implies $(c_{k-1} + 2)^2 \equiv 1 \pmod{-d_k}$, we obtain

$$(m^2 - 3n^2 + m - 3n)^2 \equiv 4(m - n)^2 \pmod{-d_k}.$$

Moreover

$$(m^2 - 3n^2 + m - 3n)^2 \equiv 4(m - n)^2 \pmod{-4d_k} \tag{4.4}$$

since $(4, d_k) = 1$ and both sides of the congruence relation are divisible by 4, since m and n are of the same parity. Under assumption $n < \frac{2}{3}\sqrt[4]{-d_k}$ one easily sees that the expressions on both sides of the congruence relation (4.4) are strictly smaller than $-4d_k$. Indeed,

$$0 \leq 2(m - n) \leq 2n\left(\sqrt{3} - 1\right) < 2\left(\sqrt{3} - 1\right)\frac{2}{3}\sqrt[4]{-d_k} < \sqrt{-4d_k}$$

and

$$0 < -m^2 + 3n^2 - m + 3n \leq 2n^2 + 2n \leq 3n^2 < \frac{12}{9}\sqrt{-d_k} < \sqrt{-4d_k}.$$

Therefore $-m^2+3n^2-m+3n = 2(m-n)$, wherefrom clearly $m \neq n$, so $m > n$. From (4.3) we obtain

$$-(c_{k-1}+2)\cdot 2(m-n) \equiv 2(m-n) \pmod{-4d_k},$$

wherefrom

$$-2s_k s_{k-1}(m-n) \equiv 3(m-n) \pmod{-2d_k}.$$

Since (2.4) implies $-2s_k^2 \equiv 1 \pmod{-d_k}$, by multiplying both sides of the previous equation by s_k we obtain

$$s_{k-1}(m-n) \equiv 3s_k(m-n) \pmod{-d_k},$$

and since $2 \mid m-n$ and $(d_k, 2) = 1$, it follows that

$$(m-n)(3s_k - s_{k-1}) \equiv 0 \pmod{-2d_k}. \tag{4.5}$$

On the other hand, from

$$0 < m-n < n\left(\sqrt{3}-1\right) < \left(\sqrt{3}-1\right)\frac{2}{3}\sqrt[4]{-d_k} < 0.49 \cdot \sqrt[4]{-d_k}$$

and

$$0 < 3s_k - s_{k-1} \leq 3s_k = 3 \cdot \sqrt{\frac{-d_k-1}{2}} < 3 \cdot \sqrt{\frac{-d_k}{2}}$$

it follows that

$$0 < (m-n)(3s_k - s_{k-1}) < 1.04 \cdot \sqrt[4]{-d_k^3} < -2d_k.$$

Therefore, we have a contradiction with (4.5). Completely analogously a contradiction can be obtained in other three cases, i.e when $\nu_m^+ = \omega_n^-$, $\nu_m^- = \omega_n^+$ and $\nu_m^- = \omega_n^-$. □

5. The application of Bennett's theorem

LEMMA 5.1. *Let*

$$\theta_1 = \sqrt{1 + \frac{1}{d_k}}, \qquad \theta_2 = \sqrt{1 + \frac{1}{3d_k}}$$

and let (x, y, z) *be a solution in positive integers of the system of Pellian equations* (2.2) *and* (2.3). *Then*

$$\max\left\{\left|\theta_1 - \frac{6s_k x}{3z}\right|, \left|\theta_2 - \frac{2t_k y}{3z}\right|\right\} < (1-d_k)z^{-2}.$$

PROOF. Clearly $\theta_1 = \frac{2s_k}{\sqrt{-2d_k}}$ and $\theta_2 = \frac{2t_k}{\sqrt{-6d_k}}$. Hence,

$$\begin{aligned}\left|\theta_1 - \frac{6s_kx}{3z}\right| &= \left|\frac{2s_k}{\sqrt{-2d_k}} - \frac{2s_kx}{z}\right| = 2s_k\left|\frac{z - x\sqrt{-2d_k}}{z\sqrt{-2d_k}}\right| \\ &= \frac{2s_k}{z\sqrt{-2d_k}} \cdot \frac{1-d_k}{z + x\sqrt{-2d_k}} < \frac{2s_k(1-d_k)}{\sqrt{-2d_k}} \cdot z^{-2} \\ &< (1-d_k)\cdot z^{-2}.\end{aligned}$$

and

$$\begin{aligned}\left|\theta_2 - \frac{2t_ky}{3z}\right| &= \left|\frac{2t_k}{\sqrt{-6d_k}} - \frac{2t_ky}{3z}\right| = \frac{2t_k}{\sqrt{3}}\left|\frac{z\sqrt{3} - y\sqrt{-2d_k}}{z\sqrt{-2d_k}\sqrt{3}}\right| \\ &= \frac{2t_k}{3z\sqrt{-2d_k}} \cdot \frac{3-d_k}{z\sqrt{3} + y\sqrt{-2d_k}} \\ &< \frac{2t_k(3-d_k)}{3\sqrt{-6d_k}} \cdot z^{-2} < \frac{3-d_k}{3} \cdot z^{-2} < (1-d_k)\cdot z^{-2}.\end{aligned}$$

□

In order to establish the lower bound for the expression in Lemma 5.1 we use the following result of Bennett [**9**] on simultaneous rational approximations of square roots of rationals which are close to 1.

THEOREM 5.2. *If a_i, p_i, q and N are integers for $0 \le i \le 2$ with $a_0 < a_1 < a_2$, $a_j = 0$ for some $0 \le j \le 2$, q nonzero and $N > M^9$ where*

$$M = \max\{|a_i| : 0 \le i \le 2\},$$

then we have

$$\max_{0\le i\le 2}\left\{\left|\sqrt{1 + \frac{a_i}{N}} - \frac{p_i}{q}\right|\right\} > (130N\gamma)^{-1}q^{-\lambda}$$

where

$$\lambda = 1 + \frac{\log(33N\gamma)}{\log\left(1.7N^2\prod_{0\le i<j\le 2}(a_i - a_j)^{-2}\right)}$$

and

$$\gamma = \begin{cases} \frac{(a_2-a_0)^2(a_2-a_1)^2}{2a_2-a_0-a_1}, & a_2 - a_1 \ge a_1 - a_0 \\ \frac{(a_2-a_0)^2(a_1-a_0)^2}{a_1+a_2-2a_0}, & a_2 - a_1 < a_1 - a_0. \end{cases}$$

We can apply Theorem 5.2 with

$$\begin{aligned} &N = -3d_k, && a_0 = -3, && a_1 = -1, && a_2 = 0, \\ &M = 3, && q = 3z, && p_1 = 6s_kx, && p_2 = 2t_ky, \end{aligned}$$

since $N = -3d_k > 3^9$ for $k \ge 6$. So,

$$\max\left\{\left|\theta_1 - \frac{6s_kx}{3z}\right|, \left|\theta_2 - \frac{2t_ky}{3z}\right|\right\} > (130\cdot(-3d_k)\gamma)^{-1}\cdot(3z)^{-\lambda},$$

where

$$\gamma = \frac{36}{5}, \qquad \lambda = 1 + \frac{\log\left(-99d_k \cdot \frac{36}{5}\right)}{\log\left(1.7 \cdot 9d_k^2 \cdot \frac{1}{36}\right)}.$$

From Lemma 5.1 we get

$$z^{-\lambda+2} < (1-d_k)\left(130 \cdot (-3d_k) \cdot \frac{36}{5}\right) \cdot 3^{\lambda}.$$

Since $\lambda < 2$ and $-d_k(1-d_k) < 1.000000821d_k^2$ for $k \geq 6$, it follows that $z^{-\lambda+2} < 25272.03d_k^2$ and hence

$$(-\lambda+2)\log z < \log\left(25272.03d_k^2\right).$$

Since

$$\frac{1}{2-\lambda} = \frac{1}{1 - \frac{\log\left(-99d_k \cdot \frac{36}{5}\right)}{\log\left(1.7 \cdot 9d_k^2 \cdot \frac{1}{36}\right)}} \leq \frac{\log\left(0.425d_k^2\right)}{\log(-0.00059d_k)}$$

we have

$$\log z < \frac{\log\left(25272.03d_k^2\right)\log\left(0.425d_k^2\right)}{\log(-0.00059d_k)}. \tag{5.3}$$

Furthermore, since $z = \nu_m^{\pm}$ for some $m \geq 0$, it follows that

$$z > \frac{1}{2}\left(-2d_k - 1 + 2s_k\sqrt{-2d_k}\right)^m.$$

Since $2s_k\sqrt{-2d_k} > -2d_k - 2$ for $k \geq 0$ it follows that

$$z > \frac{1}{2}\left(-4d_k - 3\right)^m.$$

From $(-4d_k-3)^{-1} < \frac{1}{2}$ for $k \geq 1$, we get $z > (-4d_k-3)^{m-1}$. Therefore,

$$\log z > (m-1)\log(-4d_k - 3),$$

and since $m \geq n \geq \frac{2}{3} \cdot \sqrt[4]{-d_k}$, it follows that $m - 1 > 0.5 \cdot \sqrt[4]{-d_k}$ and hence

$$\log z > 0.5 \cdot \sqrt[4]{-d_k} \cdot \log(-4d_k - 3).$$

Using (5.3) we obtain

$$\sqrt[4]{-d_k} < \frac{\log\left(25272.03d_k^2\right)\log\left(0.425d_k^2\right)}{0.5 \cdot \log(-0.00059d_k)\log(-4d_k-3)}.$$

The expression on the right side of the inequality decreases when k increases, and hence by substituting $k = 6$ we obtain

$$\sqrt[4]{-d_k} < 20.477$$

and finally

$$-d_k < 175\,817.$$

This implies $k \leq 5$, which contradicts the assumption $k \geq 6$. Therefore, the minimal integer k for which Theorem 1.6 does not hold, if such exists, is smaller than 6.

6. Small cases

To complete the proof it remains to show that Theorem 1.6 holds also for $0 \leq k \leq 5$. In each case we have to solve a system of Pellian equations where one of the equations is always the Pell's equation

$$y^2 - 3x^2 = 1$$

and the second one is as follows

- if $k = 0$ $\quad z^2 - 2x^2 = 2$,
- if $k = 1$ $\quad z^2 - 6x^2 = 4$,
- if $k = 2$ $\quad z^2 - 22y^2 = 12$,
- if $k = 3$ $\quad z^2 - 902x^2 = 452$,
- if $k = 4$ $\quad z^2 - 4182y^2 = 2092$,
- if $k = 5$ $\quad z^2 - 58242y^2 = 29122$.

All the solutions in positive integers of $y^2-3x^2 = 1$ are given by $(x, y) = (x'_m, y'_m)$, where

$$x'_m = \frac{1}{2\sqrt{3}}\left((2+\sqrt{3})^m - (2-\sqrt{3})^m\right),$$
$$y'_m = \frac{1}{2}\left((2+\sqrt{3})^m + (2-\sqrt{3})^m\right)$$

and $m \geq 0$. Likewise, we can find a sequence of solutions for any of the equations listed above. The above systems can be reduced to finding the intersections of (x'_m) and following sequences:

$$k = 0: \quad x_n = \frac{1+\sqrt{2}}{2}(3+2\sqrt{2})^n + \frac{1-\sqrt{2}}{2}(3-2\sqrt{2})^n,$$
$$k = 1: \quad x_n = \frac{1}{\sqrt{6}}(5+2\sqrt{6})^n - \frac{1}{\sqrt{6}}(5-2\sqrt{6})^n,$$
$$k = 3: \quad x_n^{\pm} = \pm\frac{61+2\sqrt{902}}{\sqrt{902}}(901 \pm 30\sqrt{902})^n,$$
$$\mp\frac{61-2\sqrt{902}}{\sqrt{902}}(901 \mp 30\sqrt{902})^n$$

that is to finding the intersections of (y'_m) and following sequences:

$$\begin{aligned}
k=2: \quad y_n^{\pm} &= \pm\frac{5+\sqrt{22}}{\sqrt{22}}(197\pm 42\sqrt{22})^n \mp \frac{5-\sqrt{22}}{\sqrt{22}}(197\mp 42\sqrt{22})^n,\\
k=4: \quad y_n^{\pm} &= \pm\frac{841+13\sqrt{4182}}{\sqrt{4182}}(37637\pm 582\sqrt{4182})^n\mp\\
&\quad \mp\frac{841-13\sqrt{4182}}{\sqrt{4182}}(37637\mp 582\sqrt{4182})^n,\\
k=5: \quad y_n^{\pm} &= \pm\frac{23419+97\sqrt{58241}}{2\sqrt{58241}}(524177\pm 2172\sqrt{58241})^n\mp\\
&\quad \mp\frac{23419-97\sqrt{58241}}{2\sqrt{58241}}(524177\mp 2172\sqrt{58241})^n,
\end{aligned}$$

with $n \geq 0$. In what follows, we will briefly resolve the case $k = 1$, so to demonstrate a method based on Baker's theory on linear forms in logarithms.

If $k = 1$ the problem reduces to finding the intersection of sequences

$$\begin{aligned}
x'_m &= \frac{1}{2\sqrt{3}}\left((2+\sqrt{3})^m-(2-\sqrt{3})^m\right)\\
x_n &= \frac{1}{\sqrt{6}}\left((5+2\sqrt{6})^n-(5-2\sqrt{6})^n\right)
\end{aligned}$$

Clearly $x'_0 = x_0 = 0$ and $x'_2 = x_1 = 4$. We have to show that there are no other intersections. Assume $m, n \geq 3$ and $x'_m = x_n$. Setting

$$P=\frac{1}{2\sqrt{3}}(2+\sqrt{3})^m, \quad Q=\frac{1}{\sqrt{6}}(5+2\sqrt{6})^n,$$

we have

$$P-\frac{1}{12}P^{-1}=Q-\frac{1}{6}Q^{-1}.$$

Since

$$Q-P=\frac{1}{6}Q^{-1}-\frac{1}{12}P^{-1}>\frac{1}{6}(Q^{-1}-P^{-1})=\frac{1}{6}P^{-1}Q^{-1}(P-Q),$$

we have $Q > P$. Furthermore, from

$$\frac{Q-P}{Q}=\frac{1}{6}Q^{-1}P^{-1}-\frac{1}{12}P^{-2}<\frac{1}{6}Q^{-1}P^{-1}+\frac{1}{12}P^{-2}<0.25P^{-2}$$

we get

$$\begin{aligned}
0<\log\frac{Q}{P}&=-\log\left(1-\frac{Q-P}{Q}\right)<\frac{Q-P}{Q}+\left(\frac{Q-P}{Q}\right)^2\\
&<\frac{1}{4}P^{-2}+\frac{1}{16}P^{-4}<0.32P^{-2}<e^{-m}.
\end{aligned}$$

The expression $\log\frac{Q}{P}$ can be written as a linear form in three logarithms in algebraic integers. Indeed

$$\Lambda:=\log\frac{Q}{P}=-m\log\alpha_1+n\log\alpha_2+\log\alpha_3,$$

with $\alpha_1 = 2+\sqrt{3}$, $\alpha_2 = 5+2\sqrt{6}$ and $\alpha_3 = \sqrt{2}$. Then $0 < \Lambda < e^{-m}$.

Now, we can apply the famous result of Baker and Wüstholz [**4**].

LEMMA 6.1. *If $\Lambda = b_1\alpha_1 + \cdots + b_l\alpha_l \neq 0$, where $\alpha_1, \ldots, \alpha_l$ are algebraic integers and $b_1, \ldots, b_l$ are rational integers, then*

$$\log|\Lambda| \geq -18(l+1)!l^{l+1}(32d)^{l+2}h'(\alpha_1)\cdots h'(\alpha_l)\log(2ld)\log B,$$

where $B = \max\{|\alpha_1|, \ldots, |\alpha_l|\}$, d is the degree of the number field generated by $\alpha_1, \ldots, \alpha_l$ over $\mathbb{Q}$,

$$h'(\alpha) = \frac{1}{d}\max\{h(\alpha), |\log\alpha|, 1\}$$

and $h(\alpha)$ denotes the logarithmic Weil height of α .

In our case $l = 3$, $d = 4$, $B = m$, $\alpha_1 = 2+\sqrt{3}$, $\alpha_2 = 5+2\sqrt{6}$ and $\alpha_3 = \sqrt{2}$. From Lemma 6.1 and from $\Lambda < e^{-m}$ we obtain

$$m \leq 2\cdot 10^{14}\log m.$$

Since the previous inequality does not hold for $m \geq M = 10^{16}$, we conclude that if there is a solution of $x'_m = x_n$ then $n \leq m < M = 10^{16}$. This upper bound can be reduced by using the following lemma, which was originally introduced in [**3**].

LEMMA 6.2 ([**28**], Lemma 4a). *Let θ, β,α, a be a positive real numbers and let M be a positive integer. Let p/q be a convergent of the continued fraction expansion of θ such that $q > 6M$. If $\varepsilon = \|\beta q\| - M\cdot\|\theta q\| > 0$, where $\|\cdot\|$ denotes the distance from the nearest integer, then the inequality*

$$|m\theta - n + \beta| < \alpha a^{-m},$$

has no integer solutions m and n such that $\log(\alpha q/\varepsilon)/\log a \leq m \leq M$.

After we apply Lemma 6.2 with $\theta = \log\alpha_1/\log\alpha_2$, $\beta = \log\alpha_3/\log\alpha_2$, $\alpha = 1/\log\alpha_2$, $M = 10^{16}$ and $a = e$, we obtain a new upper bound $M = 38$ and by another application of Lemma 6.2 we obtain $M = 7$. By examining all the possibilities, we prove that the only solutions of $x'_m = x_n$ are $x'_0 = x_0 = 0$ and $x'_2 = x_1 = 4$.

All the other cases can be treated similarly. We get these explicit results.

$$\begin{aligned}
&k = 0: && x_0 = x'_1 = 1\\
&k = 1: && x_0 = x'_0 = 0, \quad x_1 = x'_2 = 4\\
&k = 2: && y_0^+ = y'_1 = 2, \quad y_1^- = y'_3 = 26\\
&k = 3: && x_0^+ = x'_2 = 4, \quad x_1^- = x'_4 = 56\\
&k = 4: && y_0^+ = y'_3 = 26, \quad y_1^- = y'_5 = 362\\
&k = 5: && y_0^+ = y'_4 = 97, \quad y_1^- = y'_6 = 1351.
\end{aligned}$$

These can be interpreted in terms of Theorem 1.6. So, if $0 \leq k \leq 5$ and the set $\{1, 3, d_k, d\}$ is a Diophantine quadruple in $\mathbb{Z}\left[\sqrt{-2}\right]$, then $d = d_{k-1}$ or $d = d_{k+1}$, which completes the proof of Theorem 1.6.

Bibliography

1. M. Abramovitz and I. Stegun, *Handbook of mathematical functions with formulas, graphs and mathematical tables*, Dover, 1972.
2. A. Baker, *Bounds for solutions of hyperelliptic equations*, Proc. Cambridge Phil. Soc. **65** (1969), 439–444.
3. A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford **20** (1969), 129–137.
4. A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19–62.
5. A. Bazsó, D. Kreso, F. Luca, and Á. Pintér, *On equal values of power sums of arithmetic progressions*, Glas. Mat. Ser III **47(67)** (2012), 253–263.
6. A. Bazsó, Á. Pintér, and H.M. Srivastava, *A refinement of Faulhaber's theorem concerning sums of powers of natural numbers*, Appl. Math. Lett. **25** (2012), 486–489.
7. R. Beals, J. Wetherell, and M.E. Zieve, *Polynomials with a common composite*, Israel J. Math. **174** (2009), 93–117.
8. A.F. Beardon and T.W. Ng, *On Ritt's factorization of polynomials*, J. London. Math. Soc. **62** (2000), 127–138.
9. M.A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. **498** (1998), 173–200.
10. ———, *A superelliptic equation involving alternating sums of powers*, Publ. Math. Debrecen **79** (2011), 317–324.
11. Y. Bilu, *Quadratic factors of* $f(x) - g(y)$, Acta Arith. **90** (1999), 341–355.
12. Y. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér, and R.F. Tichy, *Diophantine equations and Bernoulli polynomials*, Compositio Math. **131** (2002), 173–188, With an appendix by A. Schinzel.
13. Y. Bilu and R.F. Tichy, *The Diophantine equation* $f(x) = g(y)$, Acta Arith. **95** (2000), 261–288.
14. Y.F. Bilu, T. Stoll, and R.F. Tichy, *Octahedrons with equally many lattice points*, Period. Math. Hungar. **40** (2000), 229–238.
15. J. Brillhart, *On the Euler and Bernoulli polynomials*, J. Reine Angew. Math. **234** (1969), 45–64.
16. B. Brindza, *On S-integral solutions of the equation* $y^m = f(x)$, Acta Math. Hungar. **44** (1984), 133–139.
17. E. Brown, *Sets in which* $xy + k$ *is always a square*, Math. Comp. **45** (1985), 613–620.

18. Y. Bugeaud and A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. **135** (2003), 1–10.
19. S.D. Cohen, *The irreducibility of compositions of linear polynomials over a finite field*, Compositio Math. **47** (1982), 149–152.
20. R.S. Coulter, G. Havas, and M. Henderson, *Functional decomposition of a class of wild polynomials*, J. Combin. Math. Combin. Comput. **28** (1998), 87–94.
21. ———, *On decomposition of sub-linearised polynomials*, J. Aust. Math. Soc. **76** (2004), 317–328.
22. H. Davenport, D.J. Lewis, and A. Schinzel, *Equations of the form $f(x) = g(y)$*, Quart. J. Math. Oxford Ser. **2** (1961), 304–312.
23. R. Dedekind, *Über gruppen, deren sämmtliche theiler normaltheiler sind*, Math. Ann. **48** (1897), 548–561.
24. K. Dilcher, *On a Diophantine equation involving quadratic characters*, Compositio Math. **57** (1986), 383–403.
25. F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra **28** (1974), 88–101.
26. A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III **32** (1997), 1–10.
27. ———, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51** (1997), 311–322.
28. ———, *A proof of the Hoggatt-Bergum conjecture*, Proc. Amer. Math. Soc. **127** (1999), 1999–2005.
29. ———, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.
30. A. Dujella and C. Fuchs, *Complete solution of the polynomial version of a problem of Diophantus*, J. Number Theory **106** (2004), 326–344.
31. A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. **57** (2006), 193–201.
32. A. Dujella, I. Gusić, and R.F. Tichy, *On the indecomposability of polynomials*, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **214** (2005), 81–88.
33. A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford **49** (1998), 291–306.
34. A. Dujella and R.F. Tichy, *Diophantine equations for second-order recursive sequences of polynomials*, Q. J. Math. **52** (2001), 161–169.
35. C. Elsholtz, A. Filipin, and Y. Fujita, *On Diophantine quintuples and $D(-1)$-quadruples*, to appear in Monatsh. Math.
36. H.T. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.
37. A. Filipin and Y. Fujita, *The number of Diophantine quintuples* II, Publ. Math. Debrecen **82** (2013), 293–308.
38. Z. Franušić, *On the extensibility of Diophantine triples $\{k-1, k+1, 4k\}$ for Gaussian integers*, Glas. Mat. Ser. III **43** (2008), 265–291.
39. ———, *On the extension of the Diophantine pair $\{1,3\}$ in $\mathbb{Z}\left[\sqrt{d}\right]$*, Journal of Integer Sequences **13** (2010), Article 10.9.6.
40. Z. Franušić and D. Kreso, *Nonextensibility of the pair $\{1,3\}$ to a Diophantine quintuple in $\mathbb{Z}[\sqrt{-2}]$*, J. of Comb. Number Theory **3** (2011), 151–165.
41. M.D. Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55.
42. ———, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. **17** (1973), 128–146.

43. ———, *On a theorem of Ritt and related Diophantine problems*, J. Reine Angew. Math. **264** (1974), 40–55.
44. M.D. Fried, R.M. Guralnick, and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), 157–225.
45. M.D. Fried and R.E. McRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171.
46. Y. Fujita, *The extensibility of Diophantine pair* $\{k-1, k+1\}$, J. Number Theory **128** (2008), 322–353.
47. ———, *The number of Diophantine quintuples*, Glas. Mat. Ser. III **45** (2010), 15–29.
48. D. Ghioca, T.J. Tucker, and M.E. Zieve, *Linear relations between polynomial orbits*, Duke Math. J. **161** (2012), 1379–1410.
49. P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.
50. D. Goss, *Basic structures of function field arithmetic*, vol. 35, Springer-Verlag, 1996.
51. H. Gupta and K. Singh, *On k-triad sequences*, Internat. J. Math. Sci. **5** (1985), 799–804.
52. R.M. Guralnick and J. Saxl, *Exceptional polynomials over arbitrary fields*, Algebra, arithmetic and geometry with applications, Springer, 2004, pp. 457–472.
53. R.M. Guralnick and M.E. Zieve, *Polynomials with* PSL(2) *monodromy groups*, Ann. of Math. **172** (2010), 1315–1359.
54. J. Gutierrez and D. Sevilla, *Building counterexamples to generalizations for rational functions of Ritt's decomposition theorem*, J. Algebra **303** (2006), 655–667.
55. ———, *On decomposition of tame polynomials and rational functions*, Computer algebra in scientific computing **4194** (2006), 219–226.
56. M. Henderson, *Applications of linearised and sub-linearised polynomials to information security*, Information security and privacy, Springer, 1998, pp. 227–237.
57. M. Henderson and R. Matthews, *Composition behaviour of sub-linearised polynomials over a finite field*, Finite fields: theory, applications, and algorithms, Amer. Math. Soc., 1999, pp. 67–75.
58. K. Iwasawa, *Über die endlichen Gruppen und die Verbände ihrer Untergruppen*, J. Fac. Sci. Imp. Univ. Tokyo. Sect. I. **4** (1941), 171–199.
59. D. Kreso and Cs. Rakaczki, *Diophantine equations with Euler polynomials*, Acta Arith. **161** (2013), 267–281.
60. D. Kreso and M.E. Zieve, *Invariants of functional decomposition of rational functions*, in preparation.
61. M. Kulkarni and B. Sury, *On the Diophantine equation* $x(x+1)(x+2)\dots(x+(m-1)) = g(y)$, Indag. Math. **14** (2003), 35–44.
62. ———, *Diophantine equations with Bernoulli polynomials*, Acta Arith. **116** (2005), 25–34.
63. G. Kuperberg, R. Lyons, and M.E. Zieve, *Analogues of the Jordan-Hölder theorem for transitive G-sets*, arXiv:0712.4142.
64. H.W. Lenstra and M.E. Zieve, *A family of exceptional polynomials in characteristic three*, Finite fields and applications, Cambridge Univ. Press, 1996, pp. 209–218.
65. H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. **64** (1942), 3890–400.
66. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, 1983.
67. R. Lyons and M.E. Zieve, *The rational function analogues of Ritt's decomposition theorems*, in preparation.
68. A. Medvedev and T. Scanlon, *Invariant varieties for polynomial dynamical systems*, Ann. of Math. **179** (2014), 81–177.

69. S.P. Mohatny and M.S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quart. **23** (1985), 36–44.
70. P. Müller, *New examples of exceptional polynomials*, Finite fields: theory, applications, and algorithms, Amer. Math. Soc., 1994, pp. 245–249.
71. P. Müller, *Primitive monodromy groups of polynomials*, Recent developments in the inverse Galois problem (Seattle, WA, 1993), vol. 186, Amer. Math. Soc., 1995, pp. 385–401.
72. T. Nagell, *Introduction to Number Theory*, Chelsea, 1981.
73. O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559–584.
74. ———, *Theory of non-commutative polynomials*, Ann. of Math. **34** (1933), 480–508.
75. F. Pakovich, *On polynomials sharing pre-images of compact sets and related questions*, Geom. Funct. Anal. **18** (2008), 163–183.
76. G. Péter, Á. Pintér, and A. Schinzel, *On equal values of trinomials*, Monatsh. Math. **162** (2011), 313–320.
77. Á. Pintér, *On a class of Diophantine equations related to the numbers of cells in hyperplane arrangements*, J. Number Theory **129** (2009), 1664–1668.
78. Á. Pintér and Cs. Rakaczki, *On the zeros of shifted Bernoulli polynomials*, Appl. Math. Comput. **187** (2007), 379–383.
79. H. Rademacher, *Topics in Analytic Number Theory*, Springer-Verlag, 1973.
80. Cs. Rakaczki, *On the Diophantine equation $S_m(x) = g(y)$*, Publ. Math. Debrecen **65** (2004), 439–460.
81. ———, *On the simple zeros of shifted Euler polynomials*, Publ. Math. Debrecen **79** (2011), 623–636.
82. ———, *On some generalizations of the Diophantine equation $s(1^k+2^k+\cdots+x^k)+r = dy^n$*, Acta Arith. **151** (2012), 201–216.
83. J.H. Rickert, *Simultaneous rational approximations and related Diophantine equations*, Proc. Cambridge Philos. Soc. **113** (1993), 461–472.
84. J.F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.
85. ———, *Permutable rational functions*, Trans. Amer. Math. Soc. **25** (1923), 339–448.
86. ———, *Equivalent rational substitutions*, Trans. Amer. Math. Soc. **26** (1924), 221–229.
87. J.J. Schäffer, *The equation $1^p + 2^p + 3^p + \cdots + n^p = m^q$*, Acta Math. **95** (1956), 155–189.
88. A. Schinzel, *Selected topics on polynomials*, University of Michigan Press, 1982.
89. ———, *Polynomials with special regard to reducibility*, Cambridge University Press, 2000.
90. C.L. Siegel, *Über einige Anwendungen Diophantischer Approximationes*, Abh. Preuss. Akad. Wiss. Phys.–Math. Kl. **1** (1929), 209–266.
91. T. Soundararajan, *Normal polynomials in simple extension fields.* II, Monatsh. Math. **72** (1968), 432–444.
92. T. Stoll, *Diophantine equations involving polynomial families*, Ph.D. thesis, TU Graz, 2003.
93. P. Tortrat, *Sur la composition des polynômes*, Colloq. Math. **55** (1988), 329–353.
94. U. Zannier, *Ritt's second theorem in arbitrary characteristic*, J. Reine Angew. Math. **445** (1993), 175–203.
95. M.E. Zieve, *Decompositions of Laurent polynomials*, arXiv:0710.1902.
96. M.E. Zieve and P. Müller, *On Ritt's polynomial decomposition theorems*, arXiv:0807.3578.