ON ROOTS OF UNITY IN ORBITS
OF RATIONAL FUNCTIONS

ALINA OSTAFE

(Communicated by Matthew A. Papanikolas)

Abstract. We consider a large class of univariate rational functions over a
number field \( K \), including all polynomials over \( K \), and give a precise descrip-
tion of the exceptional set of such functions \( h \) for which there are infinitely
many initial points in the cyclotomic closure \( K^c \) for which the orbit under iter-
ations of \( h \) contains a root of unity. Our results are similar to previous results
of Dvornicich and Zannier describing all polynomials having infinitely many
preperiodic points in \( K^c \). We also pose several open questions.

1. Introduction and statements

1.1. Motivation. Let \( K \) be a number field and \( h : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q}) \) a morphism
defined over \( K \). We can write \( h = f/g \in \mathbb{K}(X) \) as a rational map, where \( f, g \in \mathbb{K}[X] \)
are polynomials without common zeros. We define the \( n \)th iterate of \( h \) by
\[
h^{(0)} = X, \quad h^{(n)} = h\left(h^{(n-1)}\right), \quad n \geq 1.
\]

For an element \( \alpha \in \mathbb{P}^1(\mathbb{Q}) \) we define the orbit of \( h \) at \( \alpha \) as the set
\[
\text{Orb}_h(\alpha) = \{ h^{(n)}(\alpha) \mid n = 1, \ldots \}.
\]

We note that, whenever \( \deg f > \deg g + 1 \), the orbit \( \text{Orb}_h(\alpha) \) of an element \( \alpha \in \mathbb{Q} \) is a
finite set if for some \( n \geq 0 \), \( h^{(n)}(\alpha) \) is a pole of \( h \) (since \( \infty \) is a fixed point of \( h \) in
this case).

In this paper we are looking at the presence of roots of unity in orbits \((1.1)\)
of univariate rational functions \( h = f/g \) with \( \deg f > \deg g + 1 \). In particular, we
prove that unless the rational function is very special, there are only finitely many
initial points that are roots of unity such that the corresponding orbit contains
another root of unity. In fact our result is more general.

This work is motivated by a similar result of Dvornicich and Zannier [2, Theorem
2] that applies only for preperiodic points of univariate polynomials (for a multivari-
ate characterisation see [3, Theorem 34]). Our methods follow the same ideas and
technique of [2], including a sharp Hilbert’s irreducibility theorem for cyclotomic
extensions [2, Corollary 1] and an extension of Loxton’s result [5, Theorem 1] in
representing cyclotomic integers as short combinations of roots of unity [2, Theorem
L].

In particular, the Hilbert’s irreducibility theorem for cyclotomic extensions [2,
Corollary 1] already says that, for a rational function \( h \) over a number field \( K \), there

Received by the editors May 17, 2016 and, in revised form, July 3, 2016.
2010 Mathematics Subject Classification. Primary 11R18, 37F10.

©2016 American Mathematical Society
are finitely many preimages of roots of unity in the cyclotomic closure of \( \mathbb{K} \); see Corollary 2.2 below.

We note that a more general Hilbert irreducibility theorem over cyclotomic fields has been obtained by Zannier [8, Theorem 2.1], which may be of use for further generalisations of the results of [2] and of this paper. In Section 1.3 we suggest such a generalisation that covers these results in a unified scenario.

1.2. Notation, conventions and definitions. We use the following notation:

- \( \bar{Q} \): the algebraic closure of \( \mathbb{Q} \);
- \( U \): the set of all roots of unity in \( \mathbb{C} \);
- \( \mathbb{K} \): number field;
- \( \mathbb{K}^c = \mathbb{K}(U) \): the cyclotomic closure of \( \mathbb{K} \);
- \( |\cdot| \): the usual absolute value in \( \mathbb{C} \);
- \( C(\alpha) \): the maximum of absolute values \( |\sigma(\alpha)| \) of the conjugates \( \sigma(\alpha) \) over \( \mathbb{Q} \) of an algebraic number \( \alpha \);
- \( \mathbb{K}^c_\alpha \): the set of \( \alpha \in \mathbb{K}^c \) such that \( C(\alpha) \leq A \);
- \( T_d \): the Chebyshev polynomial of degree \( d \); it is uniquely determined by the equation \( T_d(x + x^{-1}) = x^d + x^{-d} \).

As previously mentioned, a rational function \( h = f/g \in \mathbb{K}(X) \), where \( f, g \in \mathbb{K}[X] \), is considered such that the polynomials \( f \) and \( g \) do not have common zeros.

**Definition 1.1 (Special rational functions).** We call a rational function \( h \in \mathbb{K}(X) \) special if \( h \) is a conjugate (with respect to the group action given by PGL\(_2(\mathbb{K}) \) on \( \mathbb{K}(X) \)) to \( \pm X^d \) or to \( \pm T_d(X) \).

For a rational function \( h \in \mathbb{K}(X) \), we define

\[
S_h = \{ \alpha \in \mathbb{K}^c \mid h^{(k)}(\alpha) \in U \text{ for some } k \geq 1 \}.
\]

1.3. Main results. Our goal is to prove that the set \( S_h \) is finite unless the rational function \( h \) is special. Let \( \text{Per}(h) \) be the set of the periodic points of \( h \) (that is, points which generate purely periodic orbits) and let \( \text{Preper}(h) \) be the set of the preperiodic points of \( h \) (that is, points that have a periodic point in their orbits).

If \( f \) is a polynomial, then the finiteness (under some natural conditions) of the set \( \text{Per}(f) \cap U \), which is a subset of \( S_f \), follows immediately as a very special case from a more general result of Dvornicich and Zannier [2]. More precisely, let \( f \in \mathbb{K}[X] \) be of degree at least 2. Then, by [2, Theorem 2], the set \( \text{Preper}(f) \cap \mathbb{K}^c \) is finite unless, for some linear polynomial \( L \in \mathbb{Q}[X] \) and for some \( \varepsilon = \pm 1 \), \( (L \circ f \circ L^{-1})(X) \) is either \( \varepsilon X^d \) or \( T_d(\varepsilon X) \).

Here we extend the finiteness property of \( \text{Per}(f) \cap U \) to the full set \( S_f \), as well as obtain such a result for a large class of non-special rational functions; see Definition 1.1.

**Theorem 1.2.** Let \( h = f/g \in \mathbb{K}(X) \), where \( f, g \in \mathbb{K}[X] \) with \( \deg f = d \) and \( \deg g = e \) satisfying \( d - e > 1 \). If \( f(X) - Y^m g(X) \) as a polynomial in \( X \) does not have a root in \( \mathbb{K}^c(Y) \) for all positive integers \( m \leq d \), then \( S_h \) is finite unless \( h \) is special.

We note that the degree condition \( d - e > 1 \) in Theorem 1.2 is equivalent to saying that \( \infty \) is a superattracting fixed point for \( h \).

Moreover, as remarked above, the finiteness of the set \( h(\mathbb{K}^c) \cap U \) follows directly from Hilbert’s irreducibility theorem for cyclotomic extensions [2, Corollary 1],
which we formulate in Corollary 2.2 below, without any degree restriction as in Theorem 1.2.

It is also natural to ask whether [2] Theorem 2] can be extended in full and thus investigate the finiteness of the set

(1.3) \[ T_h(A) = \{ \alpha \in \mathbb{K}^c \mid h^{(k)}(\alpha) \in \mathbb{K}^c \text{ for some } k \geq 1 \}. \]

For any rational function \( h = f/g \) satisfying the degree condition in Theorem 1.2 there is a constant \( L_h \) such that if \( C(\gamma) > L_h \), then the sequence \( C(h^{(n)}(\gamma)) \), \( n = 1, 2, \ldots \), is strictly monotonically increasing; see Section 2.2 below. Hence, we have \( \text{Preper}(h) \cap \mathbb{K}^c \subseteq T_h(L_h) \) and also \( S_h = T_h(1) \). Unfortunately some underlying tools seem to be missing in this situation.

Maybe one can start with a possibly easier problem, that is, for \( a \in \mathbb{N} \) and a rational function \( h \in \mathbb{K}(X) \), prove the finiteness of the set

\[ S_{h,a} = \{ \alpha \in \mathbb{K}(U_a) \mid h^{(k)}(\alpha) \in U_a \text{ for some } k \geq 1 \}, \]

where \( U_a = \{ t \in \overline{\mathbb{Q}} \mid t^n = a \text{ for some } n \geq 1 \} \).

2. Preliminaries

2.1. Hilbert’s irreducibility theorem over \( \mathbb{K}^c \). We need the following result due to Dvornicich and Zannier [2] Corollary 1]. We present it however in a weaker form that is needed for our results, but the proof is given within the proof of [2] Corollary 1].

**Lemma 2.1.** Let \( f \in \mathbb{K}^c[X,Y] \) be such that \( f(X,Y^m) \) as a polynomial in \( X \) does not have a root in \( \mathbb{K}^c(Y) \) for all positive integers \( m \leq \deg_X f \). Then \( f(X,\zeta) \) has a root in \( \mathbb{K}^c \) for only finitely many roots of unity \( \zeta \).

**Proof.** As we have mentioned, this statement is a part of the proof of [2] Corollary 1]: the polynomial \( g \) which appears in the proof satisfies the same condition as our polynomial \( f \) (we also note that here we alternated the roles of the variables \( X \) and \( Y \)). \( \square \)

**Lemma 2.1** implies a similar conclusion for rational functions as well, which is worth recording separately.

**Corollary 2.2.** Let \( h = f/g \in \mathbb{K}(X) \), where \( f,g \in \mathbb{K}[X] \) with \( \deg f = d \) and \( \deg g = e \). If \( f(X) - Y^m g(X) \) as a polynomial in \( X \) does not have a root in \( \mathbb{K}^c(Y) \) for all positive integers \( m \leq \max\{d,e\} \), then the set \( h(\mathbb{K}^c) \cap \mathbb{U} \) is finite.

**Proof.** We note that for any \( \zeta \in \mathbb{U} \), the set of roots in \( \mathbb{K}^c \) of \( h(X) - \xi \) is given by the set of roots in \( \mathbb{K}^c \) of the polynomial \( f(X) - \zeta g(X) \). Since by our hypothesis the polynomial \( F(X,Y) = f(X) - Yg(X) \in \mathbb{K}^c[X,Y] \) satisfies the condition of Lemma 2.1 there are finitely many \( \zeta \in \mathbb{U} \) such that \( F(X,\zeta) \) has a root in \( \mathbb{K}^c \), and thus, the conclusion follows. \( \square \)

We have the following straightforward consequence, which is needed for the proof of Theorem 1.2.

**Corollary 2.3.** Let \( f \in \mathbb{K}^c[X,Y] \) and a linear polynomial \( \mathcal{L} = aY + b \in \mathbb{K}^c[X] \) such that \( f(X,\mathcal{L}(Y^m)) \) as a polynomial in \( X \) does not have a root in \( \mathbb{K}^c(Y) \) for all positive integers \( m \leq \deg_X f \). Then \( f(X,\beta) \) has a root in \( \mathbb{K}^c \) for only finitely many elements \( \beta \in \mathcal{L}(\mathbb{U}) \).
Proof. For any \( \beta = a\zeta + b \in \mathcal{L}(\mathbb{U}) \), with \( \zeta \in \mathbb{U} \), \( f(X, \beta) \) has a root in \( \mathbb{K}^c \) if and only if \( g(X, \zeta) \) has a root in \( \mathbb{K}^c \), where \( g = f(X, aY + b) \in \mathbb{K}^c[X, Y] \). The result now follows directly from Lemma 2.1 applied with the polynomial \( g \).

2.2. Representations via linear combinations of roots of unity. Loxton [3, Theorem 1] proved that any algebraic integer \( \alpha \) contained in some cyclotomic field has a short representation as a sum of roots of unity, that is, \( \alpha = \sum_{i=1}^{b} \zeta_i \), where \( \zeta_1, \ldots, \zeta_b \in \mathbb{U} \), and \( b \leq \mathcal{R}(C(\alpha)) \) for a suitable function \( \mathcal{R} : \mathbb{R} \to \mathbb{R}_+ \). We refer to such a function \( \mathcal{R} \) as a Loxton function.

Dvornicich and Zannier [2, Theorem L] extended the result of Loxton [5, Theorem 1] to algebraic integers contained in a cyclotomic extension of a given number field, which we present below.

Lemma 2.4. There exists a number \( B \) and a finite set \( E \subset \mathbb{K} \) with \( \#E \leq [\mathbb{K} : \mathbb{Q}] \) such that any algebraic integer \( \alpha \in \mathbb{K}^c \) can be written as \( \alpha = \sum_{i=1}^{b} c_i \xi_i \), where \( c_i \in E \), \( \xi_i \in \mathbb{U} \) and \( b \leq \#E \cdot \mathcal{R}(BC(\alpha)) \), where \( \mathcal{R} : \mathbb{R} \to \mathbb{R}_+ \) is any Loxton function.

2.3. The size of elements in orbits. In this section we prove some useful simple facts about the size of iterates. In the interest of self-containment, we present all the details of the proofs of these statements, which follow by simple computations.

Lemma 2.5. Let \( f = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{K}[X] \) be of degree \( d \geq 2 \) and let \( \alpha \in \overline{\mathbb{Q}} \) be such that

\[
|\alpha|_v > \max_{j=0,\ldots,d-1} \{1, |a_j|_v\}
\]

for some non-archimidean absolute value \( |\cdot|_v \) of \( \mathbb{K} \) (normalised in some way and extended to \( \mathbb{K} = \overline{\mathbb{Q}} \)). Then \( \{f^n(\alpha)|_v\}_{n\in\mathbb{N}} \) is strictly increasing.

Proof. The proof follows by induction on \( n \geq 1 \). For \( n = 1 \) we need to prove that \( |f(\alpha)|_v > |\alpha|_v \). We note that

\[
|\alpha^d - f(\alpha)|_v \leq \max_{j=0,\ldots,d-1} |a_j \alpha^j|_v = \max_{j=0,\ldots,d-1} |a_j|_v |\alpha|^j_v < |\alpha|^d_v,
\]

where the last inequality follows from (2.1). Hence,

\[
|f(\alpha)|_v = \max\{|\alpha^d - f(\alpha)|_v, |\alpha|^d_v\} = |\alpha|^d_v.
\]

The result now follows since \( d \geq 2 \) and thus \( |\alpha|^d_v > |\alpha|_v \).

We assume now the statement is true for iterates up to \( n - 1 \). Hence for \( \beta = f^{(n-1)}(\alpha) \) we have

\[
|\beta|_v = |f^{(n-1)}(\alpha)|_v > \cdots > |f(\alpha)|_v > |\alpha|_v > \max_{j=0,\ldots,d-1} \{1, |a_j|_v\}.
\]

Using the same argument as for \( n = 1 \) with \( \beta \) instead of \( \alpha \) we obtain

\[
|f^n(\alpha)|_v = |f(\beta)|_v > |\beta|_v = |f^{(n-1)}(\alpha)|_v,
\]

which concludes the proof.

From Lemma 2.5 we also remark that any \( \alpha \in \overline{\mathbb{Q}} \) satisfying (2.1) is not a zero of the polynomial \( f \).

Corollary 2.6. Let \( h = f/g \), where \( f, g \in \mathbb{K}[X] \) are defined by

\[
f = X^d + a_{d-1}X^{d-1} + \cdots + a_0, \quad g = X^e + b_{e-1}X^{e-1} + \cdots + b_0.
\]
Let $\alpha \in \overline{\mathbb{Q}}$ be such that

$$|\alpha|_v > \max_{0 \leq i \leq d} \max_{0 \leq j \leq e} \{a_i, b_j\}$$

for some non-archimedean absolute value $|\cdot|_v$ of $\mathbb{K}$. If $d - e > 1$, then $\{h^{(n)}(\alpha)|_v\}_{n \in \mathbb{N}}$ is strictly increasing.

**Proof.** We proceed by induction over $n \geq 1$. For $n = 1$ one has to prove that $|h(\alpha)|_v > |\alpha|_v$. From the proof of Lemma 2.5 and the definition of $\alpha$, one has $|f(\alpha)|_v = |\alpha|^d_\nu$ and $|g(\alpha)|_v = |\alpha|^e_\nu$, and thus $|h(\alpha)|_v = |\alpha|^{d-e}_\nu$. In particular, from the remark after Lemma 2.5 we know that $\alpha$ is not a poly of $h$. Since $d - e > 1$, the conclusion follows for $n = 1$.

We assume now the statement is true for iterates up to $n - 1$. Hence for $\beta = h^{(n-1)}(\alpha)$ we have

$$|\beta|_v = |h^{(n-1)}(\alpha)|_v > \ldots > |h(\alpha)|_v > |\alpha|_v > \max_{0 \leq i \leq d} \max_{0 \leq j \leq e} \{a_i, b_j\}.$$ 

Using the same argument as for $n = 1$ with $\beta$ instead of $\alpha$ we obtain

$$|h^{(n)}(\alpha)|_v = |h(\beta)|_v > |\beta|_v = |h^{(n-1)}(\alpha)|_v,$$

which concludes the proof. \hfill \square

We remark that for the case $d - e \leq 1$, Corollary 2.6 does not hold. Indeed, let $\alpha \in \overline{\mathbb{Q}}$ satisfying (2.2). From the proof of Corollary 2.6 we have $|h(\alpha)|_v = |\alpha|^{d-e}_\nu$.

If $d = e$, then $|h(\alpha)|_v = 1$, and thus $\{h^{(n)}(\alpha)|_v\}_{n \in \mathbb{N}}$ is not strictly increasing (or decreasing). For example, assume $\max_{0 \leq i \leq d} \max_{0 \leq j \leq e} \{a_i, b_j\} < 1$; then $|h^{(n)}(\alpha)|_v = 1$ for all $n \geq 1$.

If $d = e + 1$, then one has $|h^{(n)}(\alpha)|_v = |\alpha|_v$, $n \geq 1$, and thus again it is not strictly increasing.

If $d - e < 0$, assume that $|a_0|_v, |b_0|_v > 1$. From the above we have $|h(\alpha)|_v = |\alpha|^{d-e}_\nu \leq |\alpha|^{-1}_\nu$, and in particular, $|h(\alpha)|_v^{-1} \geq |\alpha|_v$, which satisfies (2.2). Now, for the next iterate we have

$$|h^{(2)}(\alpha)|_v = |h(\alpha)|_v^{d-e} \frac{|f^*(h(\alpha)^{-1})|_v}{|g^*(h(\alpha)^{-1})|_v},$$

where $f^*(X) = X^df(X^{-1})$ and $g^* = X^eg(X^{-1})$ (thus, $a_0$ and $b_0$ become the leading coefficients of $f^*$ and $g^*$, respectively). Since $|h(\alpha)|_v^{-1}$ satisfies (2.2) and using the condition $|a_0|_v, |b_0|_v > 1$, simple computations as in the proof of Lemma 2.5 show that $|h^{(2)}(\alpha)|_v = |a_0|_v/|b_0|_v$, which does not tell us anything about being increasing or decreasing from the previous iterate $h(\alpha)$.

Thus, although similar ideas might work for $d - e \leq 1$, different conditions are needed to be in place to control the strict growth of iterates, which is essential for the proof of Theorem 1.2.

In the proof of Theorem 1.2 we apply Lemma 2.3 to iterates of a rational function applied in a point of $\overline{\mathbb{K}}^c$. For this reason we need to control the growth of the house of such iterates, which is presented below. However it is convenient to start with estimating the absolute value of the iterates, which is a simple application of the triangle inequality for absolute values over $\mathbb{C}$. 


Lemma 2.7. Let \( h = f/g, \) where \( f, g \in \mathbb{C}[X] \) are defined by
\[
f = X^d + a_{d-1}X^{d-1} + \cdots + a_0, \quad g = X^e + b_{e-1}X^{e-1} + \cdots + b_0.
\]
Let \( \alpha \in \mathbb{C} \) be such that
\[
|\alpha| > 1 + \sum_{i=0}^{d-1} |a_i| + \sum_{j=0}^{e-1} |b_j|.
\]
If \( d - e > 1, \) then \( \{ |h^{(n)}(\alpha)| \}_{n \in \mathbb{N}} \) is strictly increasing.

Proof. The proof goes again by induction over \( n. \) We prove only the case \( n = 1, \)
since the implication from \( n - 1 \) to \( n \) follows exactly the same lines. We have
\[
|h(\alpha)| = \frac{|f(\alpha)|}{|g(\alpha)|}.
\]

We look first at \( |f(\alpha)|. \) As above, by the triangle inequality, we have
\[
|f(\alpha)| \geq |\alpha|^d - |f(\alpha) - \alpha^d|.
\]
where the last inequality follows since \( |\alpha| \geq 1, \) we conclude that
\[
|f(\alpha)| \geq |\alpha|^{d-1} \left( |\alpha| - \sum_{i=0}^{d-1} |a_i| \right).
\]

We also have that
\[
|g(\alpha)| = |\alpha^e + b_{e-1}\alpha^{e-1} + \cdots + b_0| \leq |\alpha|^e \left( 1 + \sum_{j=0}^{e-1} |b_j| \right).
\]
Putting together (2.4) and (2.5), and recalling the initial assumption (2.3), we conclude that
\( |h(\alpha)| > |\alpha|. \) The induction step from \( n - 1 \) to \( n \) follows the same
way as for \( n = 1. \)

Corollary 2.8. Let \( h = f/g, \) where \( f, g \in \mathbb{K}[X] \) are defined by
\[
f = X^d + a_{d-1}X^{d-1} + \cdots + a_0, \quad g = X^e + b_{e-1}X^{e-1} + \cdots + b_0.
\]
Let \( A \in \mathbb{R} \) be positive and define
\[
L_h = \max_{\sigma} \left\{ 1 + \sum_{i=0}^{d-1} |\sigma(a_i)| + \sum_{j=0}^{e-1} |\sigma(b_j)|, A \right\},
\]
where the maximum is taken over all embeddings \( \sigma \) of \( \mathbb{K} \) in \( \mathbb{C}. \) Let \( \alpha \in \overline{\mathbb{Q}} \) be such
that \( C(h^{(k)}(\alpha)) \leq A \) for some \( k \geq 1. \) If \( d - e > 1, \) then \( C(h^{(\ell)}(\alpha)) \leq L_h \) for all
\( \ell < k. \)

Proof. This follows immediately from Lemma 2.7. Indeed, assume that \( d - e > 1 \)
and that \( C(h^{(\ell)}(\alpha)) > L_h \) for some \( \ell < k. \) This means that there exists a conjugate
of \( h^{(\ell)}(\alpha), \) which we denote by \( \sigma(h^{(\ell)}(\alpha)) , \) such that
\( |\sigma(h^{(\ell)}(\alpha))| > L_h. \) We note that
\( \sigma(h^{(\ell)}(\alpha)) = \sigma(h)^{\ell} \sigma(\alpha), \) where \( \sigma(h) \) is the rational function \( h \) in which
we replace the coefficients of \( f \) and \( g \) by \( \sigma(a_i) \) and \( \sigma(b_j), \) \( i = 0, \ldots, d - 1, j = 0, \ldots, e - 1. \) We apply now Lemma 2.7 with
the rational function \( \sigma(h) \) and the point \( \sigma(h^{(\ell)}(\alpha)) \) satisfying \( |\sigma(h^{(\ell)}(\alpha))| > L_h \) to conclude that \( \{ \sigma(h^{(\ell+n)}(\alpha)) \}_{n \in \mathbb{N}} \) is
strictly increasing. Thus, we obtain that \(|\sigma (h^{(k)}(\alpha))| > A\), which is a contradiction with \(C(h^{(k)}(\alpha)) \leq A\).

\[ \square \]

2.4. Growth of the number of terms in rational function iterates. The main result of the paper relies on the following result of Fuchs and Zannier [3 Corollary] which says that the number of terms in the iterates \(h^{(n)}\) of a rational function \(h \in \mathbb{K}(X)\) goes to infinity with \(n\) (see [7] for a previous result applying only to polynomials). Here is the more precise statement:

\textbf{Lemma 2.9.} Let \(q \in \mathbb{K}(X)\) be a non-constant rational function and let \(h \in \mathbb{K}(X)\) be of degree \(d \geq 2\). Assume that \(h\) is not special. Then, for any \(n \geq 3\), \(h^{(n)}(g(X))\) is a ratio of polynomials having all together at least \((n-2) \log d - \log 2016) / \log 5\) terms.

3. Proof of Theorem 1.2

We proceed first by bringing the rational function \(h\) to a monic rational function (that is, both numerator and denominator are monic polynomials). Indeed, if \(h = f/g = c\tilde{f}/\tilde{g}\) with \(c \in \mathbb{K}^*\) and \(\tilde{f}\) and \(\tilde{g}\) are monic polynomials, then there exists a linear polynomial \(L = \mu X \in \mathbb{K}[X]\) such that \(h_\mu = L \circ h \circ L^{-1}\) is monic, that is, \(\mu\) is a solution to the equation \(c\mu^{1-d+e} = 1\). Without loss of generality (enlarging the field \(\mathbb{K}\) if necessary) we can assume that \(\mu \in \mathbb{K}\).

Since \(h_\mu^{(k)} = L \circ h_\mu^{(k)} \circ L^{-1}\), we can work with the monic rational function

\[ h_\mu(X) = \frac{f_\mu(X)}{g_\mu(X)}, \]

where

\[ f_\mu(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0, \quad g_\mu(X) = X^e + b_{e-1}X^{e-1} + \cdots + b_0. \]

We are now left with proving the finiteness of the set

\[ S_{h,\mu} = \{ \alpha \in \mathbb{K}^c \mid h_\mu^{(k)}(\alpha) \in \mathbb{L}(\mathbb{U}) \text{ for some } k \geq 1 \} \]

(rather than of the set \(S_h\)).

The proof follows the approach of the proof of [2 Theorem 2], coupled with Corollary [2,3]. Indeed, by (3.1) simple computations show that \(f_\mu(X) - Y^m g_\mu(X)\) as a polynomial in \(X\) does not have a root in \(\mathbb{K}^c(Y)\) if and only if \(f(X) - Y^m g(X)\) has the same property, which is satisfied by our hypothesis. Thus, we apply Corollary [2,3] with the polynomial \(f_\mu(X) - Y g_\mu(X)\) and get that there are finitely many \(\beta \in \mathbb{L}(\mathbb{U})\) such that \(f_\mu(X) - \beta g_\mu(X)\) has a zero in \(\mathbb{K}^c\). This implies that there are finitely many \(\beta \in \mathbb{L}(\mathbb{U})\) such that \(h_\mu(X) - \beta\) has a zero in \(\mathbb{K}^c\). Denote by \(S\) the set of such \(\beta \in \mathbb{L}(\mathbb{U})\).

It is sufficient to prove that, for any \(\beta \in S\), there are finitely many \(\alpha \in \mathbb{K}^c\) such that \(h_\mu^{(k)}(\alpha) = \beta\) for some \(k \geq 1\).

Let \(A_\mu = C(\mu)\) where \(\mu \in \mathbb{K}\) is the coefficient of the above linear polynomial \(L(X) = \mu X\). Thus, for any \(\beta = \mu \xi \in \mathbb{L}(\mathbb{U})\) for some \(\xi \in \mathbb{U}\), we have \(C(\beta) = C(\mu \xi) = A_\mu\).

Let \(L_h\) be a positive integer defined as in Corollary [2,8] with \(A\) replaced by \(A_\mu\). Let also \(M\) be a sufficiently large positive integer, chosen to satisfy

\[ M > \frac{B_{h,\mathbb{K}} \log 5 + \log 2016}{\log \max\{d, e\}} + 2, \]
where \( B_{h,K} \) is defined below to be a constant depending only on \( h \) and \( K \).

If \( k < M \), then obviously there are finitely many \( \alpha \in \mathbb{K}^r \) such that \( h_{\mu}^{(k)}(\alpha) = \beta \) for any \( \beta \in S \).

We assume now \( k > M \) and we denote

\[
S_{h,\mu}(M) = \{ \alpha \in S_{h,\mu} \mid h_{\mu}^{(k)}(\alpha) \in S \text{ for some } k > M \},
\]

where as above \( \mathcal{L}(X) = \mu X \).

By Corollary 2.6 for any \( \alpha \in S_{h,\mu}(M) \) we have that \( C(h_{\mu}^{(r)}(\alpha)) \leq L_h \) for all \( r = 0, \ldots, M \).

Moreover, as in the proof of \([2, \text{Theorem 2}]\), for any \( \alpha \in S_{h,\mu}(M) \) and any non-archimidean place \( | \cdot |_v \) of \( \mathbb{K} \) (normalised in some way and extended to \( \mathbb{K} = \overline{\mathbb{F}} \)), we have that

\[
|h_{\mu}^{(r)}(\alpha)|_v \leq \max\{1, |\mu|_v, |a_j|_v, |b_j|_v \}
\]

for all \( r = 0, \ldots, M \), since otherwise, by Corollary 2.6, we see that \( \{ |h_{\mu}^{(r+n)}(\alpha)|_v \}_{n \in \mathbb{N}} \) is strictly increasing, which contradicts \( \mathcal{L}(X) = \mu X \) (and thus \( |h_{\mu}^{(k)}(\alpha)|_v = |\mu\xi|_v = |\mu|_v |\xi|_v \) for some \( \xi \in \mathbb{U} \) for some \( k > M \). Hence, taking a positive integer \( D_{h,\mu} \) such that \( D_{h,\mu}a_i \) and \( D_{h,\mu}b_j \), \( i = 0, \ldots, d - 1 \), \( j = 0, \ldots, e - 1 \), and \( D_{h,\mu} \) are all algebraic integers, we conclude that

\[
|D_{h,\mu}h_{\mu}^{(r)}(\alpha)|_v \leq \max\{|D_{h,\mu}|_v, |D_{h,\mu}\mu|_v, |D_{h,\mu}a_j|_v, |D_{h,\mu}b_j|_v \} \leq 1,
\]

and thus \( D_{h,\mu}h_{\mu}^{(r)}(\alpha) \) are all algebraic integers for any \( \alpha \in S_{h,\mu}(M) \) and \( r = 0, \ldots, M \).

Applying now Lemma 2.4 for \( D_{h,\mu}h_{\mu}^{(r)}(\alpha) \), \( r = 0, \ldots, M \), there exist a positive integer \( B_{h,\mathbb{K}} \) and a finite set \( E_{\mathbb{K}} \), depending only on \( h \) and \( \mathbb{K} \) such that, for every \( \alpha \in S_{h,\mu}(M) \) and every integer \( 0 \leq r \leq M \), we can write \( h_{\mu}^{(r)}(\alpha) \) in the form

\[
h_{\mu}^{(r)}(\alpha) = c_{r,1}\xi_{r,1} + \cdots + c_{r,B_{h,\mathbb{K}}}\xi_{r,B_{h,\mathbb{K}}}, \quad r = 0, \ldots, M,
\]

where \( c_{r,i} \in E_{\mathbb{K}} \) and \( \xi_{r,i} \in \mathbb{U} \).

Assume now that for \( M \) satisfying \((3.2)\) the set \( S_{h,\mu}(M) \) is infinite. Since for any \( \alpha \in S_{h,\mu}(M) \), \( h_{\mu}^{(r)}(\alpha) \) can be written in the form \((3.3)\), and the set \( E_{\mathbb{K}} \) is finite, we can pick an infinite subset \( T_{h,\mu}(M) \) of \( S_{h,\mu}(M) \) such that, for any \( \alpha \in T_{h,\mu}(M) \), the \( c_{r,i} \in E_{\mathbb{K}} \) in \((3.3)\) are fixed for \( i = 1, \ldots, B_{h,\mathbb{K}} \) and \( r = 0, \ldots, M \). In other words, the coefficients \( c_{r,i} \) do not depend on \( \alpha \).

As in the proof of \([2, \text{Theorem 2}]\), we may use the first equation corresponding to \( r = 0 \) to replace \( \alpha \) on the left-hand side of \((3.3)\) and thus obtain

\[
h_{\mu}^{(r)} \left( \sum_{i=1}^{B_{h,\mathbb{K}}} c_{0,i} x_{0,i} \right) = \sum_{i=1}^{B_{h,\mathbb{K}}} c_{r,i} x_{r,i}, \quad r = 1, \ldots, M.
\]

We view the points \( (\xi_{r,i}), \ i = 1, \ldots, B_{h,\mathbb{K}}, \ r = 0, \ldots, M, \) as torsion points on the variety \( Z \) defined by the equations derived from \((3.4)\) in \( \mathbb{G}^{B_{h,\mathbb{K}}(M+1)} \), and by our assumption, there are infinitely many such points.

Following the proof of \([2, \text{Theorem 2}]\), by the torsion points theorem (see \([1, \text{Theorem 4.2.2}]\)), the Zariski closure \( \overline{Z} \) of the torsion points in \( Z \) is a finite union of torsion cosets in \( \mathbb{G}^{B_{h,\mathbb{K}}(M+1)} \). Moreover, as in the proof of \([2, \text{Theorem 2}]\), the image of the map \( \varphi : \overline{Z} \to \mathbb{P}^1 \) defined on the points \( (\xi_{r,i}) \in \overline{Z} \subseteq \mathbb{G}^{B_{h,\mathbb{K}}(M+1)} \) by \( \varphi((\xi_{r,i})) = \sum_{i=1}^{B_{h,\mathbb{K}}} c_{0,i} \xi_{0,i} \), contains the infinite set \( T_{h,\mu}(M) \), and thus a dense set.
Therefore, $\mathcal{Z}$ must contain at least one torsion coset of $\mathbb{G}_m^{B_h,K}(M+1)$ of dimension 1 which is not sent to a constant by $\varphi$.

Considering this 1-dimensional torsion coset to be parametrized by $x_{r,i} = \xi_{r,i}t^{e_{r,i}}$ with a parameter $t$, where $\xi_{r,i}$ are roots of unity and $e_{r,i}$ are integers, not all zero, we obtain the following identities:

\begin{equation}
(3.5) \quad h^{(r)}_{\mu} \left( \sum_{i=1}^{B_h,K} c_{0,i} \xi_{0,i} t^{e_{0,i}} \right) = \sum_{i=1}^{B_h,K} c_{r,i} \xi_{r,i} t^{e_{r,i}}, \quad r = 1, \ldots, M.
\end{equation}

We denote by $q(t) = \sum_{i=1}^{B_h,K} c_{0,i} \xi_{0,i} t^{e_{0,i}}$, and (3.5) shows that the rational functions $h^{(r)}_{\mu}(q(t))$, $r = 1, \ldots, M$, can be represented by a rational function with at most $B_h,K$ number of terms. We apply now Lemma 2.9 and conclude that

\[ B_{h,K} \geq \frac{1}{\log 5} \left( (M - 2) \log \max\{d, e\} - \log 2016 \right), \]

which contradicts the choice of $M$ as in (3.2). This concludes the proof.

4. Comments

It would be of interest to extend the result of [2] and of this paper to the set (1.3). One important tool would be a Hilbert’s irreducibility theorem over $\mathbb{K}^c$, which for such extensions would mean to prove that under some natural conditions, a polynomial $g \in \mathbb{K}^c[X,Y]$ has the property that $g(X, \alpha)$ is reducible over $\mathbb{K}^c$ for finitely many $\alpha \in \mathbb{K}^c$ with $C(\alpha) \leq A$. One way to start investigating such a result would be to use first the Loxton theorem and represent all such $\alpha$ in the form $\eta_1 \xi_1 + \ldots + \eta_B \xi_B$, where $\eta_i \in E$, $i = 1, \ldots, B$, $B$ a positive number and $E$ a finite set that depend only on $\mathbb{K}$. We therefore reduced the problem to proving that there exist finitely many tuples $(\xi_1, \ldots, \xi_B) \in \mathcal{U}^B$ such that $C(\eta_1 \xi_1 + \ldots + \eta_B \xi_B) \leq A$ and $g(X, \eta_1 \xi_1 + \ldots + \eta_B \xi_B)$ is reducible over $\mathbb{K}^c$. Then, one may apply the multivariate version of Hilbert’s irreducibility theorem over cyclotomic fields with explicit specialisations at the set of torsion points of $\mathbb{G}_m^B$ due to Zannier; see [8, Theorem 2.1].

ACKNOWLEDGEMENTS

The author is very grateful to Umberto Zannier for suggesting that the technique used in the proof of [2, Theorem 2] would work for proving the results obtained in this paper. The author would like to thank very much Igor Shparlinski and Umberto Zannier for many useful and inspiring discussions, and for comments on an initial version of the paper. The author is also grateful to the reviewer for a careful reading of the paper and useful comments.

The research of the author was supported by the UNSW Vice Chancellor’s Fellowship.

REFERENCES


School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia

E-mail address: alina.ostafe@unsw.edu.au