A DYNAMICAL MORDELL-LANG PROPERTY ON THE DISK

MING-XI WANG

Abstract. We prove that two finite endomorphisms of the unit disk with degree at least two have orbits with infinite intersections if and only if they have a common iterate.

1. Introduction

In recent papers [8] and [9] Ghioca, Tucker and Zieve proved the following theorem: “two nonlinear polynomials have orbits with infinitely many intersections if and only if they have a common iterate.” Moreover they have observed that this is a dynamical analogue of the Mordell-Lang conjecture and have formulated a more general dynamical Mordell-Lang problem. In this paper we prove a result that fits into this context.

Let \((\text{End}(X), \circ)\), respectively \(\text{Aut}(X)\), be the monoid of finite endomorphisms, respectively the group of holomorphic automorphisms, of an analytic space \(X\), and let \(O_f(x)\) be the set of orbits of \(x \in X\) under \(f \in \text{End}(X)\). Finite endomorphisms of the unit disk are finite Blaschke products, namely rational functions of the form

\[
f(z) = \varrho \prod_{i=1}^{n} \frac{z - a_i}{1 - \overline{a_i} z}
\]

with \(\varrho\) in the unit circle \(T\), \(n \in \mathbb{N}\) and \(a_i \in E\), where \(E\) is the unit disk. In particular it follows that \(\text{End}(E) \subset \text{End}(\mathbb{P}^1)\). We shall regard a finite Blaschke product as an endomorphism of the unit disk, the unit circle, the Riemann sphere or the mirror image of the unit disk \(E^c\), depending on corresponding contexts. We shall prove:

Theorem 1.1. Pick \(\{x, y\} \subset \mathbb{P}^1\) and \(\{f, g\} \subset \text{End}(E) \setminus \text{Aut}(E)\). If \(O_f(x) \cap O_g(y)\) is infinite, then \(f\) and \(g\) have a common iterate.

Together with the work of Ghioca-Tucker-Zieve (cf. [8], [9]) we have

Theorem 1.2 (Theorem 1.1 and [9]). Let \(X\) be a simply connected open Riemann surface with the ideal boundary \(X^\partial\), and pick \(\{f, g\} \subset \text{End}(X) \setminus \text{Aut}(X)\) and \(\{x, y\} \subset X \cup X^\partial\). If the intersection \(O_f(x) \cap O_g(y)\) is infinite, then \(f\) and \(g\) have a common iterate.

Received by the editors December 20, 2013 and, in revised form, April 12, 2015 and June 16, 2015.

2010 Mathematics Subject Classification. Primary 11Z05; Secondary 37P05.

Key words and phrases. Arithmetic dynamics, fundamental group, rational points, Blaschke product, Faltings’ theorem, heights, monodromy, elliptic rational function.

The author was partially supported by a scholarship of ZGSM and the SNF grant and Austrian Science Fund(FWF): P24574.

©2016 American Mathematical Society

2183
The proof of Theorem 1.1 relies on two faces of the endomorphism monoid $(\text{End}(\mathbb{E}), \circ)$. Firstly the infiniteness of $\mathcal{O}_f(x) \cap \mathcal{O}_g(y)$ leads to very special forms of factorizations of $f^i$ and of $g^j$ in $(\text{End}(\mathbb{E}), \circ)$ for all $\{i,j\} \subseteq \mathbb{N}$. More precisely if $\mathcal{O}_f(x) \cap \mathcal{O}_g(y)$ is infinite, then for all positive integers $m, n$ there are infinitely many rational points on $\mathbb{P}^1 \times f^m, g^n \mathbb{P}^1$. Then Faltings’ theorem implies that at least one of the components of $\mathbb{P}^1 \times f^m, g^n \mathbb{P}^1$ is of genus less than two. Going further than a result of Bilu-Tichy type, our Theorem 6.2 shall imply that $f^n$ and $g^m$ indeed have very special forms of factorizations. Secondly the factorization of any element $F$ of $(\text{End}(\mathbb{E}), \circ)$, however, is very rigid. This means that $F$ cannot decompose in a flexible manner, and there always exists a fairly strong relationship between any two distinct factorizations of $F$. Now we have on the one hand $f^n$ and $g^m$ factorize specifically, and on the other hand there should be close ties between these factorizations. With a further lengthy analysis based on these two different kinds of properties we shall finally achieve that $f$ and $g$ have a common iterate, which completes the proof of the theorem.

In Section 2 we recall some preliminary results from Diophantine geometry and analytic geometry. Section 3 is devoted to the proof of our main lemma. In Section 4 we discuss elliptic rational functions, which is one major technical difficulty of this piece of work. We shall explain the rigidity in Section 5 based on a joint work with Ng [11]. The speciality result will be proved in Section 6 based on Faltings’ theorem, the Bilu-Tichy criterion, Riemann’s existence theorem, additivity of Euler characteristic, the use of a real structure and a deformation argument. In Section 7 we prove a result on heights that is used in the proof of the main theorem. Finally, in Section 8 we present the proof of our main theorem.

Throughout this paper $\mathcal{O}_f$ and $\mathcal{O}_f$, respectively, are the divisor of critical points and the set of critical values of a finite map $f$. The support of a divisor $D$ is denoted by $|D|$. The Riemann sphere, Gaussian plane, Poincaré disk and the unit circle are denoted by $\mathbb{P}^1$, $\mathbb{C}$, $\mathbb{E}$ and $\mathbb{T}$. The lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is abbreviated by $\Lambda_{\omega_1, \omega_2}$, and $\mathbb{X}$ may refer to the complex closure, algebraic closure or the complex conjugation. Write $\mathcal{C}_t, \mathcal{B}r_a$ and $\mathcal{B}r_1$ for the categories of continuous mappings of topological spaces, finite maps of analytic spaces and branched coverings of topological spaces, accordingly. Given $S$ an object of a category $\mathcal{C}$ we set $\mathcal{C}/S$ to be the category of $\mathcal{C}$-morphisms over $S$. A Chebyshev polynomial of degree $n$ is denoted by $T_n$. For any $a \in \mathbb{E}$ we let

$$\tau_a(z) = (z+a)/(1+\overline{a}z).$$

The 2-torsion points of an elliptic curve $E$ are denoted by $E[2]$. A curve of type $(g, \nu)$ is of genus $g$ and of $\nu$ points at infinity.

2. FACTS FROM DIOPHANTINE AND ANALYTIC GEOMETRY

Integral points of a complex irreducible projective curve $X$ are potentially dense if there exists a field $k$ of finite type over $\mathbb{Q}$ such that $X(k)$ is infinite, while integral points of a complex affine curve $X$ of type $(g, \nu)$ are potentially dense if there exists $R$ of finite type over $\mathbb{Z}$ and an affine curve $Y$ over $R$ such that $Y(\mathbb{C})$ is birational to $X$ and $Y(R)$ is infinite. We collect celebrated theorems of Siegel and of Faltings in

**Theorem 2.1** (Siegel [14], Faltings [7]). Integral points of an algebraic curve $X$ of type $(g, \nu)$ are potentially dense if and only if $\chi(X) = 2 - 2g - \nu \geq 0$. 
There are only four types of curves with nonnegative Euler characteristic, namely ones of
\[(0,0), (0,1), (0,2) \text{ and } (1,0).\]

In [9] the authors call a curve of type \((0,1)\) or \((0,2)\) a Siegel factor as Siegel’s theorem applies to them. Similarly we shall call a curve of type \((0,0)\) or \((1,0)\) a Faltings factor as Faltings’ theorem applies here.

A holomorphic map between Riemann surfaces is finite if and only if it is non-constant and proper. A holomorphic map \(f: M \to N\) between Riemann surfaces is finite if and only if there exists an integer \(n\) such that \(f(z) = c\) has \(n\) solutions for any point \(c\) of \(N\). We shall define the number \(n\) given above to be the degree of \(f\) and denote it by \(\text{deg } f\). We point out that there are no finite maps between \(\mathbb{C}\) and \(\mathbb{E}\), which is a consequence of Liouville’s theorem and

Lemma 2.2. If there exists a finite map \(f: \mathbb{E} \to N\), then \(N\) is biholomorphic to \(\mathbb{E}\).

For a proof we refer to [11]. We shall need

Lemma 2.3 ([13]). Let \(\mathcal{D}\) be a discrete subset of \(N\) and let \(q \in N \setminus \mathcal{D}\). There is a one-to-one correspondence between finite maps \(f: (M, p) \to (N, q)\) of degree \(n\) with \(\mathcal{D}_f \subset \mathcal{D}\) and subgroups \(H\) of \(\pi_1(N \setminus \mathcal{D}, q)\) of index \(n\) given by \(f \mapsto H = \pi_1(M \setminus f^{-1}(\mathcal{D}), p)\).

A finite map \(f: M \to N\) is called linear if \(\text{deg } f = 1\), and a nonlinear finite map \(f\) is called factorized (resp. prime or irreducible) if there exist (resp. do not exist) nonlinear finite maps \(g: T \to N\) and \(h: M \to T\) for which \(f = gh\). The factorizability of a polynomial, as observed by Ritt in [12], is determined by the action of fundamental groups. By Lemma 2.3 we slightly generalize this fact to finite maps.

Theorem 2.4 (Ritt [12], Ng-Wang [11]). Let \(f: M \to N\) be a finite map, \(q \in N \setminus \mathcal{D}_f\) and \(p \in f^{-1}(q)\). The map \(f\) is factorized if and only if there exists a proper intermediate group between \(\pi_1(M \setminus f^{-1}(\mathcal{D}_f), p)\) and \(\pi_1(N \setminus \mathcal{D}_f, q)\).

This simple fact suggests the rigidity of the decomposition of finite maps. Let \(f: M \to N\) be a finite map of degree \(n\) and \(q \in N \setminus \mathcal{D}_f\). The natural group homomorphism \(\rho: \pi_1(N \setminus \mathcal{D}_f, q) \to S_n\) is called the monodromy, and the image of \(\rho\) is called the monodromy group of \(f\). With an additional assumption there is an even stronger rigid property than the one stated in Theorem 2.4. Writing \(\mathcal{L}_n = \{t \in \mathbb{N} : t \mid n\}\) for the lattice that \(i \leq j\) if and only if \(i \mid j\), we have

Theorem 2.5 (Ritt [12], Ng-Wang [11]). Let \(f: M \to N\) be a finite map and let \(q \in N \setminus \mathcal{D}_f\). If there exists \(\alpha \in \pi_1(N \setminus \mathcal{D}_f, q)\) such that the monodromy action of \(\alpha\) is transitive, then the lattice of intermediate groups between \(\pi_1(M \setminus f^{-1}(\mathcal{D}_f), p)\) and \(\pi_1(N \setminus \mathcal{D}_f, q)\) is a sublattice of \(\mathcal{L}_{\text{deg } f}\).

A finite map can be recovered from their monodromy by the “Schere und Kleister” surgery [13, p. 41], and this is a well-known result of Riemann.

Theorem 2.6 (Riemann’s existence theorem). Let \(N\) be a Riemann surface, \(\mathcal{D} \subset N\) a discrete subset, \(q \in N \setminus \mathcal{D}\) and \(\rho: \pi_1(N \setminus \mathcal{D}, q) \to S_n\) a transitive representation. There exists a unique pointed finite map \(f: (M, p) \to (N, q)\) between Riemann surfaces with the monodromy of \(f\) given by \(\rho\).
We call the following group homomorphism $\rho_T: F_2 = \langle \sigma, \tau \rangle \to S_n$ a Chebyshev representation: if $n=2k$, then
\[
\rho_T(\sigma) = (2, 2k)(3, 2k-1) \cdots (k, k+2),
\]
\[
\rho_T(\tau) = (2, 1)(3, 2k) \cdots (k+1, k+2),
\]
and if $n=2k+1$, then
\[
\rho_T(\sigma) = (2, 2k+1)(3, 2k) \cdots (k+1, k+2),
\]
\[
\rho_T(\tau) = (2, 1)(3, 2k+1) \cdots (k+1, k+3).
\]

If $X$ is a simply connected Riemann surface and $p, q$ is any pair of distinct points in $X$, then $\pi_1(X \setminus \{p, q\})$ is a free group of rank 2. Using Theorem 2.6 with $\rho_T: \mathbb{C} \setminus \{p, q\} \to S_n$ (resp. $\rho_T: E \setminus \{p, q\} \to S_n$) gives elements in $\text{End}(\mathbb{C})$ (resp. $\text{End}(E)$). The former are polynomials associated to $T_n$, and the latter are called Chebyshev-Blaschke products. This construction appeared in [15] and [11]. Let $k$ be the classical elliptic modulus function as defined in [6, p. 99]; then we set $\gamma(t) = k^{\frac{1}{2}} (4ti/\pi)$. In [11] (or [15]) we have proved that

**Proposition 2.7** (Ng-Wang). Given $t > 0, n \in \mathbb{N}$ there is a unique $T_{n, t} \in \text{End}(\mathbb{E})$ that is characterized by properties that $T_{n, t}^{-1} [-\gamma(nt), \gamma(nt)] = [-\gamma(t), \gamma(t)]$ and that $T_{n, t}(\gamma(t)) = \gamma(nt)$. These $T_{n, t}$ are Chebyshev-Blaschke products. If $f$ is a Chebyshev-Blaschke product of degree $n$, then there exist $\{\epsilon, \varepsilon\} \subset \text{Aut}(\mathbb{E})$ and $t > 0$ such that $f = \epsilon \circ T_{n, t} \circ \varepsilon$.

These $T_{n, t}$ are called normalized Chebyshev-Blaschke products.

3. **The main lemma**

We shall make use of the following version of Riemann’s covering principle as given in [11] pp. 119-120. Here a Riemann surface is a pair $(X, \phi)$ with $X$ a connected Hausdorff space and $\phi$ a complex structure; see [11] p. 144. However we shall simply write $\mathbb{E}$ and $\mathbb{C}$ when $\phi$ is the canonical one.

**Theorem 3.1** (Riemann’s covering principle). Let $f: X_1 \to X_2$ be a covering surface and let $\phi_2$ be a complex structure on $X_2$. Then there exists a unique complex structure $\phi_1$ on $X_1$ such that $f: (X_1, \phi_1) \to (X_2, \phi_2)$ is holomorphic.

Let $i_0 \in \text{Hom}_{\mathbb{E}}(\mathbb{E}, \mathbb{C})$ and $f \in \text{End}(\mathbb{E})$. Theorem 3.1 applied to $i_0 \circ f: \mathbb{E} \to \mathbb{C}$ gives a new complex structure $\phi$ on $\mathbb{E}$ and a finite map $(\mathbb{E}, \phi) \to \mathbb{C}$. The classical uniformization theorem together with Lemma 2.2 shows that $(\mathbb{E}, \phi)$ must be the complex plane. Writing $i_1: \mathbb{E} \to (\mathbb{E}, \phi) = \mathbb{C}$ for the topological identity map, there exists a holomorphic map $(i_1, i_0)_* f$ which makes the diagram

\[
\begin{array}{ccc}
\mathbb{E} & \xrightarrow{f} & \mathbb{E} \\
\downarrow{i_1} & & \downarrow{i_0} \\
\mathbb{C} & \xrightarrow{(i_1, i_0)_* f} & \mathbb{C}
\end{array}
\]

commutative. We shall call $i_1$ an $f$-lifting of $i_0$ and $(i_1, i_0)_* f$ a $(i_1, i_0)$-descent of $f$. 

2186  MING-XI WANG
The uniqueness in Theorem 3.1 implies that if \( i, i' \) are two \( f \)-liftings of \( i_0 \), then there exists a holomorphic isomorphism \( \sigma: \mathbb{C} \to \mathbb{C} \) such that \( \sigma \circ i = i' \). This gives

**Corollary 3.2.** Let \( i_0 \in \text{Hom}_{\mathcal{E}_1}(\mathbb{E}, \mathbb{C}) \), \( f \in \text{End}(\mathbb{E}) \) and \( i, i' \) both be \( f \)-liftings of \( i_0 \). There exists \( \sigma \in \text{Aut}(\mathbb{C}) \) which makes the diagram

\[
\begin{array}{ccc}
\mathbb{E} & \xrightarrow{f} & \mathbb{E} \\
\downarrow{i_1} & & \downarrow{i_1'} \\
\mathbb{C} & \xrightarrow{(i_1, i_0) \circ f} & \mathbb{C}
\end{array}
\]

commutative.

Note that \( (i_1, i_0) \circ f \) and \( (i_1', i_0) \circ f \) are finite self maps of \( \mathbb{C} \) and therefore are given by polynomials. The above discussions remain true if we interchange \( \mathbb{E} \) with \( \mathbb{C} \), and then one may check easily the following simple fact.

**Proposition 3.3.** Let \( i_0 \in \text{Hom}_{\mathcal{E}_1}(\mathbb{E}, \mathbb{C}) \) and \( \{f_1, f_2\} \subset \text{End}(\mathbb{C}) \) such that \( f = f_1 \circ f_2 \). If \( i_1 \), respectively \( i_2 \), is an \( f_1 \)-lifting of \( i_0 \), respectively an \( f_2 \)-lifting of \( i_1 \), then \( i_2 \) is an \( f \)-lifting of \( i_0 \) and \( (i_2, i_0) \circ f = (i_1, i_0) \circ f_1 \circ (i_2, i_1) \circ f_2 \), as a relation in \( (\text{End}(\mathbb{E}), \circ) \).

Given \( \{f, g\} \subset \text{End}(\mathbb{E}) \) the curve \( \mathbb{P}^1 \times f, g \mathbb{P}^1 \) is a double of \( \mathbb{E} \times f, g \mathbb{E} \). Indeed, setting \( X' \), \( X \), \( X^{\mathcal{E}} \) and \( X' \) for \( \mathbb{P}^1 \times f, g \mathbb{P}^1 \), \( \mathbb{E} \times f, g \mathbb{E} \), \( T \times f, g T \) and \( \mathbb{E}^{\mathcal{E}} \times f, g \mathbb{E}^{\mathcal{E}} \) we shall have

\[
X' = X \cup X^{\mathcal{E}} \cup X'.
\]

Take \( i \in \text{Hom}_{\mathcal{E}_1}(\mathbb{E}, \mathbb{C}) \) and let \( j_1 \in \text{Hom}_{\mathcal{E}_1}(\mathbb{E}, \mathbb{C}) \) (resp. \( j_2 \in \text{Hom}_{\mathcal{E}_1}(\mathbb{E}, \mathbb{C}) \)) be an \( f \)-lifting (resp. \( g \)-lifting) of \( i \). Setting \( X_* = \mathbb{C} \times (j_1, i) \circ f, (j_2, i) \circ g \mathbb{C} \) we will compare algebraic components of the projective curve \( X' \) with those of the affine curve \( X_* \). It would be helpful to have in mind that \( X' \), \( X \) and \( X_* \) are fibrations over \( \mathbb{P}^1, \mathbb{E} \) and \( \mathbb{C} \), accordingly. This implies that \( X' \) is a double of \( X \) and \( X_* \) equals \( X \) in topology. Our main lemma gives an arithmetic reflection of these simple facts.

**Main Lemma 3.4.** There is a one-to-one correspondence between Faltings factors of \( X' \) and Siegel factors of \( X_* \).

**Proof.** We shall establish bijections from analytic components of \( X \) firstly to algebraic components of \( X' \), and secondly to algebraic components of \( X_* \).

If \( Y \) is an analytic component of \( X \), then \( Y' := \{(x, y)|((1/x, 1/y) \in Y)\} \) is an analytic component of \( X' \), as \( (x, y) \in X \iff (1/x, 1/y) \in X' \). The algebraic irreducible component \( Y' \) of \( X' \) which contains \( Y \) is given by \( Y \cup Y' \), and the correspondence given by \( Y \mapsto Y' \) is the first bijection as wanted.

Now set \( Y_* = \{(j_1(x), j_2(y))|(x, y) \in Y\} \), which is a subset of \( X_* \). The analytic structure involved is topological in nature, and therefore \( Y_* \) is also an analytic (and algebraic) component of \( X_* \). Here \( Y \mapsto Y_* \) gives our second bijection.

In the first bijection \( Y' \) is a double of \( Y \) which leads to \( \chi(Y') = 2\chi(Y) \). In the second one \( Y_* \) is topologically equivalent to \( Y \), and this gives \( \chi(Y_*) = \chi(Y) \). Finally we have \( \chi(Y'*) = 2\chi(Y_*) \), which together with Theorem 2.1 of Siegel and of Faltings proves our assertion.

\[\square\]
To handle normalized Chebyshev-Blaschke products \( T_{n,t} \subset \text{End}(\mathbb{E}) \) recalled in Section 2, we shall treat them as descents of isogenies of elliptic curves.

The construction of Chebyshev-Blaschke products (cf. [11]) relies on the representation of fundamental groups. Indeed Zolotarev constructed (cf. [18]) much earlier another family of functions by using Jacobian elliptic functions, which was called Zolotarev fractions by Bogatyrev (cf. [5]) or elliptic rational functions by scientists working in filter designs (cf. [10]). In [11] we slightly generalized Zolotarev’s original construction and obtained a larger family of rational functions \( T_{n,\tau} \) \( (n \in \mathbb{N}, \tau \in \mathbb{H}) \) by descents of cyclic isogenies of elliptic curves, where Zolotarev’s fractions correspond to \( T_{n,\tau} \) with \( \tau \) purely imaginary. We verified in [11] that there is a canonical bijection between \( T_{n,t} \) \( (t > 0) \) and \( T_{n,\tau} \) \( (\tau \text{ purely imaginary}) \). Two entirely different constructions, via elliptic functions (resp. fundamental groups) taken by Zolotarev (resp. Ng-Wang), finally lead to essentially the same class of functions.

The use of descents of cyclic isogenies of elliptic curves is originally due to Zolotarev, but he only considered Jacobian elliptic integrals (or functions) with real modulus \( k \), which prevented him from constructing a larger and universal family. For classical special functions such as \( \omega_1, \omega_2, \varepsilon_1, \cos \), \( dn \) we refer to [6] Chapter VII, and for more details of the following construction we refer to [11]. For \( \tau \in \mathbb{H} \) we denote by \( E_\tau \), respectively \( E'_\tau \), for elliptic curve \( \mathbb{C}/\Lambda_{1,\tau} \), respectively \( \mathbb{C}/\Lambda_{2,\omega_1(\tau),\omega_2(\tau)} \). Writing \( \varphi_\tau \), respectively \( \text{cd}_\tau = \cos/dn \), for the Weierstrass function on \( E_\tau \), respectively the Jacobian \( \text{cd} \) function on \( E'_\tau \), they are of order 2. There are natural cyclic isogenies \([n]: E_\tau \to E_{n\tau} \) and \([n]: E'_\tau \to E'_{n\tau} \), and according to the theory of descent we write \( n_\tau \) and \( T_{n,\tau} \) for the rational functions which make the following diagrams commutative.

Henceforth an **elliptic rational function** refers to an \( f \in \text{End}(\mathbb{P}^1) \) that satisfies \( f \sim n_\tau \) in \( (\text{End}(\mathbb{P}^1), \circ) \) for some \( (n, \tau) \in \mathbb{N} \times \mathbb{H} \). This notion is more general than the one used by engineers (cf. [10]). We have that \( T_{n,\tau} \) is elliptic because \( T_{n,\tau} \sim n_{\tau/2} \), which will be called **generalized Zolotarev fractions**. The principal result of this section is that \{Elliptic rational functions of degree \( n \geq 3 \}/ \sim \) is \( Y_0(n) \), and we begin with

**Lemma 4.1.** If \( \tau \in \mathbb{H} \) and if \( n \geq 3 \), then
\[
\circ_{n_\tau} = \varphi_{n_\tau}(E_{n\tau}[2]) \quad \text{and} \quad n_\tau^{-1}(\circ_{n_\tau}) \backslash |\mathcal{O}_{n_\tau}| = \varphi_\tau(E_\tau[2]).
\]

**Proof.** This follows from a calculation of local ramification degree. \[\square\]

Then we prove

**Theorem 4.2.** Pick \( \tau_1, \tau_2 \in \mathbb{H} \) and pick \( n \geq 3 \). Then \( n_{\tau_1} \sim n_{\tau_2} \) in \( (\text{End}(\mathbb{P}^1), \circ) \) if and only if \( \Gamma_0(n) \tau_2 = \Gamma_0(n) \tau_1 \), where
\[
\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \bigg| c \equiv 0 \pmod{n} \right\}
\]
is the modular group.
Proof. Write $e_i(\tau)$ for $e_i$ with respect to the pair of primitive periods $(1, \tau)$. First of all we show that for any pair $(n, \tau) \in \mathbb{N} \times \mathbb{H}$ and $0 \leq i \leq 3$ there exist $(\iota, \epsilon) \in \text{Aut}(\mathbb{P}^1)$ such that $n_\tau = \iota \circ n_\tau \circ \epsilon^{-1}$ and $\iota(e_i(\tau)) = e_0(\tau)$. We only verify this claim for $i = 1$ since similar arguments apply to other situations. The map $\iota: E_\tau \to E_\tau$ defined by $\iota(z) = z + 1/2$ descends to $\iota \in \text{Aut}(\mathbb{P}^1)$ with respect to $\varphi_\tau$, and the map $\epsilon: E_{n_\tau} \to E_{n_\tau}$ given by $\epsilon(w) = w + n/2$ descends to $\epsilon \in \text{Aut}(\mathbb{P}^1)$ with respect to $\varphi_{n_\tau}$:

One checks easily that $\epsilon^{-1} \circ n_\tau \circ \iota = n_\tau$ and $\iota(e_0) = e_1$, which proves the desired claim.

By construction we have $n_\tau \circ \varphi_\tau = \varphi_{n_\tau} \circ [n]$ where $[n]$ maps $E_\tau$ to $E_{n_\tau}$ for $1 \leq i \leq 2$. If there exist $\{\iota, \epsilon\} \subset \text{Aut}(\mathbb{P}^1)$ such that $\epsilon \circ n_\tau \circ \iota^{-1} = n_\tau$, then $\epsilon$ induces a bijection between $\varphi_{n_\tau_1}(E_{n_\tau_1} [2])$ and $\varphi_{n_\tau_2}(E_{n_\tau_2} [2])$, because $\iota_{n_\epsilon} = \varphi_{n_\tau_1}(E_{n_\tau_1} [2]) = \varphi_{n_\tau_2}(E_{n_\tau_2} [2])$ as $n \geq 3$. Moreover $\epsilon^{-1}$ induces a bijection between $n_{\tau_2}^{-1}(\iota_{n_\tau_2})$ (resp. $\Omega_{n_{\tau_2}}$) and $\iota_{n_\tau_1}^{-1}(\iota_{n_\tau_1})$ (resp. $\Omega_{n_{\tau_1}}$), and then we deduce from Lemma [11, 1] that $\iota^{-1}$ also induces a bijection between $\varphi_{\tau_2}(E_{\tau_2} [2])$ and $\varphi_{\tau_1}(E_{\tau_1} [2])$. The monodromy representation of a small loop around any critical value of $\varphi$ is an involution, and consequently the map $\epsilon \in \text{Aut}(\mathbb{P}^1)$ lifts to an isomorphism $\varphi_{\tau_2}(E_{\tau_2} [2]) \to \varphi_{\tau_1}(E_{\tau_1} [2])$ such that $\varphi_{\tau_2} \circ \varphi_{\tau_2}^{-1} = \varphi_{\tau_1} \circ \varphi_{\tau_1}^{-1}$ (resp. $\varphi_{\tau_2} \circ \varphi_{\tau_2}^{-1}$). By the claim made in the previous paragraph we may assume $\epsilon^{-1}(e_0(\tau_2)) = e_0(\tau_1)$, hence $\epsilon(0) = 0$ and $\epsilon^{-1}(z) = \gamma z$ with $\gamma \in \mathbb{C}^*$ and with $\epsilon^{-1}$ giving a bijection between $\Lambda_1, \tau_2$ (resp. $\Lambda_1, \tau_1$) and $\Lambda_1, \tau_2$ (resp. $\Lambda_1, \tau_1$) with $\epsilon^{-1}(E_{\tau_1} [2]) = \Lambda_{1/2n, 1/2}$ and $\Lambda_1, \tau_1$ (resp. $\Lambda_1, \tau_2$) and $\Lambda_1, \tau_2$ (resp. $\Lambda_1, \tau_1$) with $\epsilon^{-1}(E_{\tau_1} [2]) = \Lambda_{1/2n, 1/2}$. Writing $\gamma = c \tau_1 + d$ and $\gamma = c \tau_1 + d$ with $(a/b, c/d) \in \text{SL}_2(\mathbb{Z})$, by using $\tau_2 / \tau_1 = \Lambda_{1/2n, 1/2}$ we have $c \tau_1 + d \in \Lambda_{1/2n, 1/2}$ and therefore $n|c$. This verifies that $(a/b, c/d) \in \Gamma_0(n)$.

It remains to check that $n_{\tau_2} \sim n_{\tau_1}$ when $\tau_2 = (a/b, c/d) \tau_1$ with $(a/b, c/d) \in \Gamma_0(n)$:

Set $\gamma = c \tau_1 + d$. Then the map $\varphi_{\tau_2} : z \in E_{\tau_1} \mapsto z / \gamma \in E_{\tau_2}$ is an isomorphism and descends to $\varphi_{n_{\tau_2}} : z \in E_{\tau_1} \mapsto z / \gamma \in E_{n_{\tau_2}}$ in the sense that $\varphi_{n_{\tau_2}} \varphi_{\tau_2} = \varphi_{n_{\tau_1}} \circ \varphi_{\tau_1}$. Moreover $\varphi_{\tau_2} : z \in E_{n_{\tau_1}} \mapsto z / \gamma \in E_{n_{\tau_2}}$ is also an isomorphism (here we use $n(c)$) and descends to $\epsilon \in \text{Aut}(\mathbb{P}^1)$ in the sense that $\varphi_{n_{\tau_2}} \varphi_{\tau_2} = \varphi_{n_{\tau_1}} \circ \varphi_{\tau_1}$. One checks readily that $\epsilon \circ n_{\tau_1} = n_{\tau_2} \circ \epsilon$.

In [11] we have proved that

$$T_{n, \tau}(z) = \sqrt{k(4nti/\pi)} T_{n, 4ti/\pi}(z/\sqrt{k(4ti/\pi)}).$$
By using \cite{[11]}, Theorem \ref{thm4.2} and the injectivity of \( i \mathbb{R}_{>0} \hookrightarrow \Gamma_0(n) \setminus \mathbb{H} \) we have for \( t_1, t_2 > 0 \):

**Corollary 4.3.** Let \( n \geq 3 \). Then \( \mathcal{T}_{n, t_1} \sim \mathcal{T}_{n, t_2} \) in \((\text{End}(\mathbb{P}^1), \circ)\) if and only if \( t_1 = t_2 \).

We shall indicate that Theorem \ref{thm2.5} is applicable to all elliptic rational functions.

**Lemma 4.4.** Let \( f : M \to N \) be a finite map and let \( \alpha \) be a closed cycle on \( N \) over which \( f \) is unramified. If \( f^{-1}(\alpha) \) is connected, then the monodromy action of \( \alpha \) is transitive.

**Proof.** It is almost the definition. \( \square \)

We write \( C_\tau \) for the Jordan curve on \( \mathbb{P}^1 \) which is given by \( \varphi_\tau(\{ z : \Im z = \Im \tau / 4 \}) \).

**Proposition 4.5.** Given \( \tau \in \mathbb{H} \) and given \( n \in \mathbb{N} \), there exists a closed cycle \( \alpha \) on \( \mathbb{P}^1 \), along which \( n_\tau \) is unramified, such that its monodromy action is transitive.

**Proof.** By definition we have \( n_\tau^{-1}(C_\tau) = C_\tau \), and our previous lemma applies. \( \square \)

The nesting property of Zolotarev’s fractions are important in engineering, and for general elliptic rational functions we have

**Proposition 4.6** (Nesting property). Given \( m, n \in \mathbb{N} \), \( \tau \in \mathbb{H} \) and \( t > 0 \) we have

\[
(mn)_\tau = mn_\tau \circ n_\tau, \quad \mathcal{T}_{mn, \tau} = \mathcal{T}_m, n_\tau \circ \mathcal{T}_n, \tau \quad \text{and} \quad \mathcal{T}_{mn, t} = \mathcal{T}_m, n_\tau \circ \mathcal{T}_n, t.
\]

One checks easily that \( f \in \text{End}(\mathbb{E}) \) is elliptic if and only if it is a Chebyshev-Blaschke product. For any elliptic \( f \in \text{End}(\mathbb{E}) \) there exists \( t > 0 \) such that \( f \sim \mathcal{T}_{n, t} \) in \((\text{End}(\mathbb{E}), \circ)\). We set \( \chi(f) = nt \) when \( f \) is of degree at least three, which is well-defined by Theorem \ref{thm4.2} and will be called the *moduli* of \( f \).

5. Rigidity of monoid factorizations

The main result of \cite{[11]} implicitly gives generators of relations of \((\text{End}(\mathbb{E}), \circ)\).

**Theorem 5.1** (Ng-Wang). The monoid \((\text{End}(\mathbb{E}), \circ)\) is presented by \((S \mid R)\) where \( S \) consists of linear and of prime finite Blaschke products and \( R \) consists of:

\begin{itemize}
  \item[(i)] \( \iota \circ f = g \) or \( f \circ \iota = g \) where \( \iota \in \text{Aut}(\mathbb{E}) \);
  \item[(ii)] \( \tau^* g(z)^k \circ z^k = z^k \circ \tau^* g(z)^k \) with \( (k, \tau) = 1 \);
  \item[(iii)] \( \mathcal{T}_{p, q, t} \circ \mathcal{T}_{q, t} = \mathcal{T}_{q, p, t} \circ \mathcal{T}_{p, t} \) with \( p, q \) primes and \( t \) a positive real number.
\end{itemize}

We call a relation \( a \circ b = c \circ d \) with \( \deg a = \deg d \) and \( (\deg a, \deg b) = 1 \) in terms of irreducible (resp. not necessary irreducible) elements a *Ritt (resp. generalized Ritt)* relation of \((\text{End}(X), \circ)\). Presentations of monoids in Theorem \ref{thm5.1} involves only Ritt relations. The next result also follows from \cite{[11]}.

**Theorem 5.2** (Ng-Wang). If \( a \circ b = c \circ d \) is a generalized Ritt relation in \((\text{End}(\mathbb{E}), \circ)\), then up to units of \((\text{End}(\mathbb{E}), \circ)\) and up to the permutation \( a \leftrightarrow c, b \leftrightarrow d \) we are in the case \( z^s g(z)^n \circ z^n = z^n \circ z^s g(z^n) \) \((m, s) = 1\) or \( \mathcal{T}_{m, nt} \circ \mathcal{T}_{n, t} = \mathcal{T}_{m, nt} \circ \mathcal{T}_{n, t} \) \((m, n) = 1, t > 0\).

We call \( f \in \text{End}(\mathbb{E}) \) totally ramified if \( f \sim z^n \) in \((\text{End}(\mathbb{E}), \circ)\). The following simple remark is a complement of the above theorem.

**Lemma 5.3.** Let \( h \in \text{End}(\mathbb{E}) \) satisfy \( h(0) \neq 0 \) and let \( \{ s, n \} \subset \mathbb{N} \) satisfy \( n \geq 2 \). Then neither \( z^s h(z)^n \) nor \( z^s h(z^n) \) is totally ramified.
In this section we will prove, via action of fundamental groups, some rigidity properties of factorizations of \((\text{End}(\mathbb{E}), \circ)\). The following generalizes a result of [17].

**Proposition 5.4.** Let \(f: M \to N\) be a finite map of degree \(n\), \(q \in N \setminus \partial_f\) and \(\alpha \in \pi_1(N \setminus \partial_f, q)\). If finite maps \(b: M \to A; a: A \to N; d: M \to R; c: R \to N\) satisfy \(a \circ b = c \circ d = f\) and if the monodromy action of \(\alpha\) is transitive, then there exist Riemann surfaces \(T, W\) and finite maps \(h: M \to T; \overline{b}: T \to A; \overline{a}: T \to R\) such that \(deg\ g = (deg\ a, deg\ c)\) and \(deg\ h = (deg\ b, deg\ d)\) and the diagram

![Diagram](image)

commutes.

**Proof.** By Theorem 2.3 the lattice of groups intermediate between \(\pi_1(N \setminus \partial_f)\) and \(\pi_1(M \setminus f^{-1}(\partial_f))\) is isomorphic to a sublattice of \(\mathcal{L}_n\), and by Lemma 2.3 it suffices to verify the following: if \(\mathcal{L}\) is a sublattice of \((\mathcal{L}_n, \leq)\) and contains \(a\) and \(b\), then it also contains \((a, b)\) and \([a, b]\). Indeed this follows immediately from the definition of sublattice, and it can be illustrated by the figure

![Diagram](image)

where we use \(s \to t\) to denote \(s \leq t\) (for lattice structure) or equivalently \(t|s\). \(\square\)

**Proposition 5.5.** Let \(a, b, c, d, f\) be finite Blaschke products that satisfy \(a \circ b = c \circ d = f\). There exist \([\overline{a}, \overline{b}, \overline{c}, \overline{d}, h, g]\) \(\subset \text{End}(\mathbb{E})\) such that

1. \(g \circ \overline{a} = a, \ g \circ \overline{c} = c,\ deg\ g = (deg\ a, deg\ c)\);
2. \(\overline{b} \circ h = b, \ \overline{d} \circ h = d,\ deg\ h = (deg\ b, deg\ d)\);  
3. \(a \circ \overline{b} = c \circ \overline{d}\).

**Proof.** We regard these finite Blaschke products as finite maps \(E \to E\), for which the monodromy action of any loop closely around the unit circle is transitive. By Lemma 2.2 the decomposition of finite Blaschke products into finite Blaschke products is essentially equivalent to that of finite Blaschke products into finite maps. Now we may apply Proposition 5.4 directly to deduce the desired assertion. \(\square\)

We give a simple example to explain how the above rigidity applies.

**Corollary 5.6.** Let \(f: M \to N\) be a finite map that satisfies the monodromy condition required in Proposition 5.4. If there are decompositions of \(f\) into finite maps \(f = a \circ b = c \circ d\) with \(deg\ a = deg\ c\), then there exist biholomorphic maps \(\iota\) such that

\[ a = c \circ \iota^{-1}, \quad b = \iota \circ d.\]
Proof. Applying Proposition 5.4, we obtain suitable \(a, b, c, d, h\) and \(g\). Because \(\deg a = \deg c\) and \(\deg b = \deg d\) it is clear that \(a, b, c, d\) are all biholomorphic maps. One may choose \(t = \zeta^{-1} \circ \zeta\) to fulfill the desired assertion. \(\square\)

For totally ramified maps we have

**Corollary 5.7.** If \(f \in \text{End}(E)\) is of degree \(s \geq 2\) and if \(f^t\) is totally ramified for some integer \(t \geq 2\), then there exist \(p \in \text{End}(E)\) and \(\rho \in \text{T}\) such that \(f = t_p \circ \rho z^{s} \circ t_{-p}\).

Proof. By assumption there exist \(\{\epsilon, \varepsilon\} \subset \text{Aut}(E)\) such that \(f^t = \epsilon \circ z^t \circ \varepsilon\), which gives
\[
f \circ f^{t-1} = (\epsilon \circ z^t) \circ (z^{s-1} \circ \varepsilon).
\]
This together with Corollary 5.6 implies that \(f \sim \epsilon \circ z^t\) in \((\text{End}(E), \circ)\) and therefore \(f\) is totally ramified. Writing \(p = \delta f\) and \(q = |\Delta f|\) we have \(p = q\); otherwise \(f^t\) fails to be totally ramified. This gives readily \(f = t_p \circ \rho z^{s} \circ t_{-p}\) for some \(\rho \in \text{T}\). \(\square\)

For Chebyshev-Blaschke products we have

**Corollary 5.8.** If \(f \in \text{End}(E)\) is of degree \(s \geq 2\) and if \(n \geq 3\), then \(f^n\) is not elliptic.

Proof. If there exist \(\{\epsilon, \varepsilon\} \subset \text{Aut}(\mathbb{P}^1)\) and \(t > 0\) such that \(f^n = \epsilon \circ T_{s^n, t} \circ \varepsilon\), then it follows from Proposition 4.6 that
\[
\begin{align*}
f^2 \circ f^{n-2} &= (\epsilon \circ T_{s^2, s^{n-2}t}) \circ (T_{s^{n-2}, t} \circ \varepsilon) \\
f^{n-2} \circ f^2 &= (\epsilon \circ T_{s^{n-2}, s^2t}) \circ (T_{s^2, t} \circ \varepsilon).
\end{align*}
\]
Proposition 4.5 enables us to apply Corollary 5.6 to \(f^n\) and obtain that \(f^2\) is associated to both \(T_{s^2, s^{n-2}t}\) and \(T_{s^2, t}\). This leads to \(T_{s^2, s^{n-2}t} \sim T_{s^2, t}\), which contradicts Corollary 4.3 because \(s^{n-2}t\) is greater than \(t\). \(\square\)

**Corollary 5.9.** Let \(f\) be an elliptic rational function and let \(f = a \circ b\) be a relation in \((\text{End}(\mathbb{P}^1), \circ)\). Then \(a\) and \(b\) are both elliptic.

Proof. Let \(m = \deg a\) and let \(n = \deg b\). There exist \(\{\epsilon, \varepsilon\} \subset \text{Aut}(\mathbb{P}^1)\) and \(\tau \in \mathbb{H}\) such that \(f = \epsilon \circ (mn)_\tau \circ \varepsilon\), and it follows from the nesting property, Proposition 4.6, that
\[
a \circ b = (\epsilon \circ m_{\tau^2}) \circ (n_{\tau} \circ \varepsilon).
\]
Proposition 4.5 together with Corollary 5.6 gives the ellipticity of \(a\) and \(b\). \(\square\)

Zieve-Müller discovered in [17] Theorem 1.4 a new property of \((\text{End}(\mathbb{C}), \circ)\), and we shall prove that the phenomenon of Zieve-Müller remains true in \((\text{End}(E), \circ)\).

**Theorem 5.10.** Let \(\{a, b, f\} \subset \text{End}(E),\ n = \deg f \geq 2\) and \(k \in \mathbb{N}\) satisfy \(a \circ b = f^k\). If there exists no \(\iota \in \text{Aut}(E)\) for which \(\iota \circ f \circ \iota^{-1} = z^n\) and no \(g \in \text{End}(E)\) for which either \(a = f \circ g\) or \(b = g \circ f\), then \(k \leq \max \{8, 2+2\log_2 n\}\).

The proof of Theorem 5.10 relies on techniques developed in Zieve-Müller’s original work, and therefore our arguments are largely similar to those in [17], except for the manipulation of elliptic rational functions. We will be sketchy at many places.

**Lemma 5.11.** Let \(a \circ b = c \circ d\) be a generalized Ritt relation in \((\text{End}(E), \circ)\) with \(b\) (resp. \(a\)) neither totally ramified nor elliptic. We have \(\deg a < \deg b\) (resp. \(\deg b < \deg a\)).

Proof. This follows immediately from Theorem 5.2. \(\square\)
Lemma 5.12. Given $h \in \text{End}(E)$ with $h(0) \neq 0$ and coprime positive integers \( \{s, n\} \) with \( n \geq 2 \), if \( z^s h(z)^n \) or \( z^s h(z^n) \) is elliptic, then we must have \( n=2 \) and \( s=1 \).

Proof. Let \( f = z^s h(z)^n \) satisfy the above conditions; then \( 0 \in \mathcal{D}_f \). There exists \( p \in |\mathcal{D}_f| \) with \( f(p) = 0 \) and \( \mathcal{D}_f \geq n(p) \). Because \( f \) is elliptic we have \( n=2 \). If \( s \geq 2 \), then we have \( \mathcal{D}_f \geq s(0) \), which together with the ellipticity of \( f \) forces \( s=2 \). This contradicts \( (s, n) = 1 \).

Let \( f = z^s h(z^n) \) satisfy the above conditions. Take one nonzero \( x \in |\mathcal{D}_f| \) and take a primitive \( n \)-th root of unity \( \xi_n \). Then \( \xi_n^k x \in |\mathcal{D}_f| \) for all \( 0 \leq i \leq n-1 \). By ellipticity \( |\mathcal{D}_f| \) lie on a geodesic of \( E \), with respect to the Poincaré metric. Therefore \( n=2 \). For the same reason as above we have \( s=1 \). \( \square \)

Corollary 5.13. If \( a \circ b = c \circ d \) is a generalized Ritt relation in \( (\text{End}(E), \circ) \) and if \( b \) (or \( a \)) is elliptic with degree at least three, then \( a \circ b = c \circ d \) is elliptic.

Proof. Otherwise we are in the first case of Theorem 5.12 with \( a = z^n, b = z^s g(z^n) \) (or \( a = z^s g(z^n), b = z^n \)). Lemma 5.12 forces \( n=2 \) and \( s=1 \), and this can be checked easily. \( \square \)

A complete presentation \( \mathcal{U} \) of \( f \in \text{End}(E) \setminus \text{Aut}(E) \) refers to a tuple \((u_1, \ldots, u_r)\) of irreducible elements of \( (\text{End}(E), \circ) \) such that \( f = u_1 \circ \cdots \circ u_r \). If \( \mathcal{U} = (u_1, \ldots, u_r) \), \( \mathcal{V} = (v_1, \ldots, v_r) \) are complete presentations of \( f \), then by Theorem 5.1 we can pass from \( \mathcal{U} \) to \( \mathcal{V} \) by finitely many Ritt relations, and this gives a unique permutation \( \sigma_{\mathcal{U}, \mathcal{V}} \) of \( \{1, 2, \ldots, r\} \) which satisfies \( \deg u_i = \deg v_{\sigma_{\mathcal{U}, \mathcal{V}}(i)} \). In addition we have

Lemma 5.14. If \( i < j \) and if \( \sigma_{\mathcal{U}, \mathcal{V}}(i) > \sigma_{\mathcal{U}, \mathcal{V}}(j) \), then \( \deg u_i, \deg u_j = 1 \).

Following [17] we define \( \mathcal{L}(U, V, i, j) = \prod_{k<i, \sigma(k)<\sigma(j)} \deg u_k, L_{R}(U, V, i, j) = \prod_{k<i, \sigma(k)>\sigma(j)} \deg u_k, R_{L}(U, V, i, j) = \prod_{k>i, \sigma(k)<\sigma(j)} \deg u_k \) and \( R_{R}(U, V, i, j) = \prod_{k>i, \sigma(k)>\sigma(j)} \deg u_k \). Let \( \mathcal{U} = (u_1, \ldots, u_r) \) be a complete presentation of an \( f \in \text{End}(E) \setminus \text{Aut}(E) \) and let \( u_k \in \mathcal{U} \) be elliptic with \( \deg u_k \geq 3 \). The length of \( u_k \) with respect to \( \mathcal{U} \), denoted by \( h_{\mathcal{U}}(u_k) \) or \( h(u_k) \) if without ambiguity, is defined as \( h_{\mathcal{U}}(u_k) = \prod_{i=1}^{k-1} \deg u_i \). If \( u_i \) is elliptic, then according to Theorem 5.1 so is \( v_{\sigma_{\mathcal{U}, \mathcal{V}}(i)} \).

Lemma 5.15. If \( u_i \) is elliptic with degree at least three, then

\[
h(u_i) \chi(u_i) = h(v_{\sigma_{\mathcal{U}, \mathcal{V}}(i)}) \chi(v_{\sigma_{\mathcal{U}, \mathcal{V}}(i)}).
\]

Proof. This follows from Corollary 5.13, Proposition 4.6 and Corollary 5.6. \( \square \)

Moreover we also have

Lemma 5.16. If \( i < j \) and if \( \{u_i, u_j, u_i \circ u_{i+1} \circ \cdots \circ u_j \sim \mathcal{T}_{n, t}\} \subset \text{End}(E) \) are all elliptic and of degree at least three, then

\[
h(u_i) \chi(u_i) = h(u_j) \chi(u_j).
\]

Proof. Writing \( \deg u_i = d_i \), by Corollary 5.6 we have \( u_j \) (resp. \( u_i \)) is associated to \( \mathcal{T}_{d_i, t} \) (resp. \( \mathcal{T}_{d_i, r} \)), with \( r = t \prod_{k=i+1}^{j} d_k \), and therefore \( \chi(u_j) = d_j t \) and \( \chi(u_i) = d_i r \). It is also clear that \( h(u_j) = \prod_{k=i}^{j} d_k \) and \( h(u_i) = 1 \). The claim follows readily. \( \square \)

Proposition 5.17. Let \( f \in \text{End}(E) \setminus \text{Aut}(E) \), \( \mathcal{U} = (u_1, \ldots, u_r) \) and \( \mathcal{V} = (v_1, \ldots, v_r) \) be its complete presentations and \( 1 \leq k \leq r \). Writing \( \mathcal{L} = \mathcal{L}(\mathcal{U}, \mathcal{V}, k, k) \) and \( \mathcal{L}_R, \mathcal{R}_L, \mathcal{R}_R \) analogously, then \( \mathcal{L}_R, \mathcal{L}_L \) are both coprime to \( \deg u_k \) and there exist
finite Blaschke products $a$ with degree $LL$, $d$ with degree $RR$, $b, \bar{b}, \bar{d}$ with degree $LR$, $c, \bar{c}$ with degree $RL$ and $\bar{u}, \bar{u}$ with degree $\deg u_k$ such that

(i) $u_1 \circ u_2 \cdots \circ u_{k-1} = a \circ b$ and $u_{k+1} \circ \cdots \circ u_r = c \circ d$;
(ii) $bc \circ u_k = \bar{u} \circ \bar{b}$;
(iii) $\bar{u} \circ b \circ c = c \circ \bar{u} \circ \bar{b}$;
(iv) $u_k \circ c = \bar{c} \circ u$.

Proof. Based on Proposition 5.5, some analysis similar to that in the proof of Proposition 4.2 applies to our case.

Proof of Theorem 5.10 We assume that $k \geq 2$. Choose $U = (u_1, \ldots, u_r)$ to be a complete presentation of $f$. Then $U^k = (u_1, \ldots, u_{kr})$ is a complete presentation of $f^k$ where $u_i = u_{i-r}$. Let $V = (v_1, \ldots, v_{kr})$ be a complete presentation of $f^k$ for which $a = v_1 \circ v_2 \cdots \circ v_k$ and $b = v_{e+1} \cdots \circ v_{kr}$. By the assumption that $f^k = a \circ b$ and that there exists $g \in \End(E)$ for which $a = f \circ g$ or $b = g \circ f$, Proposition 5.5 applies and leads to $\deg f \mid \deg k$ and $\deg f \mid \deg b$. Therefore there exists $1 \leq m \leq r$ (resp. $1 \leq l \leq r$) such that $\sigma_{U^k, V}(m + tr) > e$ for all $0 \leq t \leq k-1$ (resp. $\sigma_{U^k, V}(l + tr) \leq e$ for all $0 \leq t \leq k-1$). Otherwise Proposition 5.5 leads to a contradiction. Moreover by Lemma 5.14 we have $(\deg u_m, \deg u_l) = 1$.

Case (i). There exists $1 \leq p \leq r$ such that $u_p$ is not associated to $z^n$, $T_{n,t}$, $z^sh(z^n)$ or $z^s h(z^n)$ in $(\End(E), \circ)$ with $h \in \End(E)$, $h(0) \neq 0$ and $n \geq 2$.

We claim that $k = 2$. Otherwise we have $k \geq 3$. On the one hand we deduce from Theorem 5.2 that $u_{p+r}$ never changes under Ritt relations and therefore $\sigma_{U^k, V}(i) < p+r$ for all $i < p+r$ and $\sigma_{U^k, V}(i) > p+r$ for all $i > p+r$, which leads to $\sigma_{U^k, V}(m) < p+r$ and $\sigma_{U^k, V}(l+(k-1)r) > p+r$. On the other hand we have $\sigma_{U^k, V}(m) > e$ and $\sigma_{U^k, V}(l+(k-1)r) \leq 0$. Consequently $e < p+r$ and $p+r < e$, a contradiction.

Case (ii). There exists $1 \leq p \leq r$ such that $u_p$ is neither totally ramified nor elliptic, but associated to $z^s h(z^n)$ or $z^s h(z^n)$ in $(\End(E), \circ)$ with $h \in \End(E)$, $h(0) \neq 0$ and $n \geq 2$.

There exists $0 \leq q \leq k-1$ for which $\sigma_{U^k, V}(p+qr) \leq e$ and $\sigma_{U^k, V}(p+(q+1)r) > e$. Because $\sigma_{U^k, V}(m + tr) > e$ for all $0 \leq t \leq q-1$ Proposition 5.17 gives

$$(\deg u_m)^q \mid LR(p+qr).$$

Similarly, because $\sigma_{U^k, V}(u_{l+tr}) \leq e$ for all $q+2 \leq l \leq k-1$ we have

$$(\deg u_l)^{k-q-2} \mid RL(p+(q+1)r).$$

By Lemma 5.11 and by Proposition 5.17 we have

$$(\deg u_m)^q < \deg u_p, \quad (\deg u_l)^{k-q-2} < \deg u_p.$$ 

This gives $2^{k-2} \leq (\deg u_p)^2 \leq n^2$, and therefore $k \leq 2 + 2 \log_2 n$ as desired.

Case (iii). All $u_i : E \to E$ in $U$ are totally ramified. If $|D_{u_i}| = d_{u_i+1} = p$ holds for all integers $i$ with $1 \leq i \leq kr-1$, then $u_p \circ t_{u_{kr}} = \zeta z^n$ for some $\zeta \in T$, which contradicts the assumption. Hence there exists $1 \leq p \leq r$ such that $|D_{u_p}| \neq d_{u_{p+1}}$. It is clear from Theorem 5.2 and from Lemma 5.3 that any Ritt relation $a \circ b \circ c = d \circ d$ in totally ramified finite Blaschke products must satisfy $d_a = d_c$ and $|D_b| = |D_d|$. This implies that if $i \leq r+p$ (resp. $(k-2)r+p+1 \leq i$), then $\sigma_{U^k, V}(i) \leq r+p$ (resp. $\sigma_{U^k, V}(i) \geq (k-2)r+p+1$), which leads to $\sigma_{U^k, V}(m) \leq r+p$ and $\sigma_{U^k, V}((k-1)r+l) \geq (k-2)r+p+1$. Using $\sigma_{U^k, V}(m) > e$ and $\sigma_{U^k, V}((l+(k-1)r) \leq e$, we obtain $e < p+r$ and $(k-2)r+p+1 \leq e$ which forces $k \leq 2.$
Case (iv). There exist $1 \leq p \leq r$ such that $u_p$ is elliptic and is of degree at least three. We claim that $k \leq 8$. Otherwise $k \geq 9$ and either $\sigma_{U^k, V}(4r+p) \leq e$ or $\sigma_{U^k, V}(4r+p) > e$.

In the former case we deduce from Proposition 5.17 that there exist $\{a, \bar{b}, \hat{b} \} \subset \text{End}(E)$ such that $\deg b = \deg \bar{b} = LR(U^k, V, p+4r, p+4r) = \hat{n}$, $\deg \bar{u} = \deg \hat{u}$ and

$$u_1 \circ u_2 \circ \cdots \circ u_{p+4r-1} = a \circ b,$$

$$b \circ u_{p+4r} = \hat{u} \circ \bar{b}.$$ 

Because $\sigma_{U^k, V}(r+m) > \sigma_{U^k, V}(m) > e \geq \sigma_{U^k, V}(4r+p)$ we have $\deg b = \hat{n} \geq 4$, and because $b \circ u_{p+4r} = \hat{u} \circ \bar{b}$ is a generalized Ritt relation, Corollary 5.13 implies that $b$ is elliptic. If we write $\hat{n} = LR(U^k, V, p+2r, p+4r)$, $h = u_1 \circ u_2 \circ \cdots \circ u_{p+2r-1}$ and $g = u_p \circ u_{p+2r+1} \circ \cdots \circ u_{p+4r-1}$, then apparently

$$a \circ b = h \circ g,$$

and for the same reason as that for $\hat{n}$ we have $\hat{n} \geq 4$. By Proposition 5.5 there exist $\{b, \hat{g}, k, e, \hat{a}, \hat{h} \} \subset \text{End}(E)$ with $\deg k = (\hat{n} = \deg b, \deg g)$, $\deg e = (\deg a, \deg h)$ and

$$\hat{b} \circ k = b, \quad \hat{g} \circ k = g,$$

$$e \circ \hat{a} = a, \quad e \circ \hat{h} = h,$$

$$\hat{a} \circ \hat{b} = \hat{h} \circ \hat{g}.$$ 

We denote $\deg k$ by $s$ and consider the generalized Ritt relation $\hat{h} \circ \hat{g} = \hat{a} \circ \hat{b}$. Because

$$\hat{n}/\hat{n} = \prod_{p+2r \leq i \leq p+4r-1, \sigma_{U^k, V}(i) > \sigma_{U^k, V}(p+4r)} \deg u_i$$

and for all $p+2r \leq i \leq p+4r-1$,

$$(\deg u_i, \hat{n}) > 1 \Rightarrow \sigma_{U^k, V}(i) > \sigma_{U^k, V}(p+4r),$$

we have $(\deg g/\hat{n}, \hat{n}) = 1$, and therefore $s = (\hat{n}, \deg g) = \hat{n}/\hat{n}$ or equivalently

$$\deg k = \prod_{p+2r \leq i \leq p+4r-1, \sigma_{U^k, V}(i) > \sigma_{U^k, V}(p+4r)} \deg u_i.$$ 

Because $\sigma_{U^k, V}(p+2r) < \sigma_{U^k, V}(p+3r) < \sigma_{U^k, V}(p+4r)$ the above equality leads to $\deg \hat{g} \geq 4$. The ellipticity of $b$ implies that of $\hat{b}$. Noticing that $\deg \hat{b} = \deg b/\deg k = \hat{n}/\deg k$ and $\deg k = \hat{n} \circ \hat{n}$, we have $\deg \hat{b} = \hat{n} \geq 4$. Considering the generalized Ritt relation $\hat{h} \circ \hat{g} = \hat{a} \circ \hat{b}$ Corollary 5.13 implies the ellipticity of $\hat{g}$. We now examine

$$g = u_p \circ u_{p+2r+1} \circ \cdots \circ u_{p+4r-1} = \hat{g} \circ k$$

and we write $\mathcal{T} = (\mathcal{P}_1 = u_p, \ldots, \mathcal{P}_{2r} = u_{p+4r-1})$, which is a complete presentation of $g$. If $\mathcal{V} = (v_1, \ldots, v_{2r})$ is a complete presentation of $g$ for which $\hat{g} = v_1 \circ v_2 \circ \cdots \circ v_o$ and $k = v_o \circ \cdots \circ v_2$, then $\sigma_{\mathcal{P}, \mathcal{V}}(1) \leq o$ and $\sigma_{\mathcal{P}, \mathcal{V}}(1+r) \leq o$. Lemma 5.10 gives

$$h(v_{\sigma_{\mathcal{P}, \mathcal{V}}(1)}) \chi(v_{\sigma_{\mathcal{P}, \mathcal{V}}(1)}) = h(v_{\sigma_{\mathcal{P}, \mathcal{V}}(1+r)}) \chi(v_{\sigma_{\mathcal{P}, \mathcal{V}}(1+r)}).$$

Then we apply Lemma 5.15 and have

$$h(\mathcal{P}_1) \chi(\mathcal{P}_1) = h(\mathcal{P}_{1+r}) \chi(\mathcal{P}_{1+r}).$$

This is impossible since $\chi(\mathcal{P}_1) = \chi(\mathcal{P}_{1+r}) = \chi(u_p)$ and $h(\mathcal{P}_1) < h(\mathcal{P}_{1+r})$.

Similar arguments apply to the case that $\sigma_{U^k, V}(4r+p) > e$. □
Corollary 5.18. Let \( f \in \text{End}(E) \setminus \text{Aut}(E) \), \( \{a, b\} \subset \text{End}(E) \) and \( l \geq 1 \) that satisfy \( a \circ b = f^l \) and there exists no \( \iota \in \text{Aut}(E) \) for which \( \iota \circ f \circ \iota^{-1} = z_{\text{deg}} f \). Then there exist \( \{\alpha, \beta\} \subset \text{End}(E) \) and nonnegative integers \( k \leq \max(8, 2 + 2 \log_2 \text{deg} f) \), \( i, j \) such that
\[
a = f^i \circ \alpha, \quad b = \beta \circ f^j, \quad \alpha \circ \beta = f^k.
\]

Proof. Let \( i \) (resp. \( j \)) be the maximal nonnegative integer such that \( a = f^i \circ \alpha \) (resp. \( b = \beta \circ f^j \)) for some \( \alpha \) (resp. \( \beta \)) in \( \text{End}(E) \). We have \( f^i \circ \alpha \circ \beta \circ f^j = f^l \) and therefore \( f^i \circ \alpha \circ \beta = f^{l-j} \). This together with Corollary 5.19 implies that there exists \( \epsilon \in \text{Aut}(E) \) for which
\[
f^i = f^i \circ \epsilon^{-1}, \quad \alpha \circ \beta = \epsilon \circ f^{l-i-j}.
\]
Replacing \( \alpha \) by \( \epsilon^{-1} \circ \alpha \) we have \( a = f^i \circ \alpha, b = \beta \circ f^j \) and \( \alpha \circ \beta = f^k \). The maximality of \( i, j \) together with Theorem 5.10 leads to \( k \leq \max(8, 2 + 2 \log_2 \text{deg} f) \). \( \square \)

As a further corollary we have

Corollary 5.19. Let \( f \in \text{End}(E) \setminus \text{Aut}(E) \) such that there exists no \( \iota \in \text{Aut}(E) \) for which \( \iota \circ f \circ \iota^{-1} = z_{\text{deg}} f \). Then there is a finite subset \( S \) such that if two finite Blaschke products \( r \) and \( s \) satisfy \( r \circ s = f^l \), then the following assertions are satisfied:

(i) either there exists \( h \in \text{End}(E) \) for which \( r = f \circ h \) or there exists \( \iota \in \text{Aut}(E) \) for which \( r \circ \iota \in S \);

(ii) either there exists \( h \in \text{End}(E) \) for which \( s = h \circ f \) or there exists \( \iota \in \text{Aut}(E) \) for which \( \iota \circ s \in S \).

Proof. We only prove the first assertion as a similar argument applies to the second one. If there exists no \( h \in \text{End}(E) \) for which \( r = f \circ h \), then Corollary 5.18 implies that \( r \) is a left factor of \( f^k \) for some \( k \leq \max(8, 2 + 2 \log_2 \text{deg} f) \). Up to associations there are only finitely many such factors. \( \square \)

6. Speciality of monoid factorizations

If the fiber product \( \mathbb{P}^1 \times_{f,g} \mathbb{P}^1 \) admits special arithmetical or geometric properties for rational functions \( f \) and \( g \), then \( f \) and \( g \) tend to have very special factorizations in \( (\text{End}(\mathbb{P}^1), \circ) \). We shall call this sort of fact the speciality of monoid factorizations. The goal of this section is to obtain speciality of factorizations of \( (\text{End}(E), \circ) \) under assumptions of finiteness of rational points. We begin with recalling the complex analytic version of the famous Bilu-Tichy criterion (cf. [3]).

Theorem 6.1 (Bilu-Tichy). Let \( f \) and \( g \) be nonlinear polynomials such that \( \mathbb{C} \times_{f,g} \mathbb{C} \) has a Siegel factor. Then \( f \) and \( g \) admit the factorizations
\[
f = \epsilon \circ f_1 \circ \epsilon, \quad g = \epsilon \circ g_1 \circ \epsilon
\]
in \( (\text{End}(\mathbb{C}), \circ) \) where \( \{\epsilon, \epsilon\} \subset \text{Aut}(\mathbb{C}) \) and there exist \( \{m, n\} \subset \mathbb{N} \) together with \( p \in \mathbb{C}[z] \setminus \{0\} \) such that \( \{f_1, g_1\} \) falls into one of the following cases:

(i) \( \{z^m, z^r p(z)^m\} \) with \( r \geq 1 \) and \( (r, m) = 1 \);

(ii) \( \{z^2, (z^2 + 1)p(x)^2\} \);

(iii) \( \{T_m, T_n\} \) with \( m \geq 3, n \geq 3 \) and \( (m, n) = 1 \);

(iv) \( \{T_m, -T_n\} \) with \( m \geq 3, n \geq 3 \) and \( (m, n) > 1 \);

(v) \( \{(z^2 - 1)^3, 3z^4 - 4z^3\} \).
In this section we shall prove

**Theorem 6.2.** If the curve \( \mathbb{P}^1 \times f, g \mathbb{P}^1 \) defined by \( \{ f, g \} \subset \text{End}(E) \) has a Faltings factor, then \( f \) and \( g \) admit the factorizations

\[
f = \epsilon \circ f_1 \circ \epsilon, \quad g = \epsilon \circ g_1 \circ \epsilon
\]

in \( \text{End}(E, \circ) \) where \( \{ \epsilon, \epsilon \} \subset \text{Aut}(E) \) and there exist positive integers \( m, n \) and \( p \in \text{End}(E) \cup \{ 1 \} \) such that \( \{ f_1, g_1 \} \) falls into one of the following cases:

(i) \( \{ z^m, z^r p(z)^m \} \) with \( r \geq 1 \) and \( (r, m) = 1 \);

(ii) \( \{ z^2, z(z - a)/(1 - \bar{a}z)p(z)^2 \} \) with \( a \in \mathbb{E} \setminus \{ 0 \} \);

(iii) \( \{ T_{m, nt}, T_{m, mt} \} \) with \( t > 0 \), \( m \geq 3, n \geq 3 \) and \( (m, n) = 1 \);

(iv) \( \{ T_{m, nt}, T_{m, mt} \} \) with \( t > 0 \), \( m \geq 3, n \geq 3 \) and \( (m, n) > 1 \);

(v) \( \{ (z^2 - a^2)/(1 - \bar{a}^2 z^2)^2, z^3(z - b)/(1 - \bar{b}z) \} \) where \( a, b \) are points in \( E \) and \( a, b, \bar{a}, \bar{b} \) satisfy an algebraic relation.

**Proof.** Follow the notation used before Lemma 3.4 and write

\[
\overline{f} := (j_1, i_1)_* f, \quad \overline{g} := (j_2, i_2)_* g.
\]

By definition we have \( f = i_1^\dagger \circ \overline{f} \circ j_1, g = i_1^\dagger \circ \overline{g} \circ j_2 \), which also means that \( j_1^{-1} \) is an \( \overline{f} \)-lifting of \( i_1^\dagger \). If \( \mathbb{P}^1 \times f, g \mathbb{P}^1 \) has a Faltings factor, then by Lemma 3.4 the curve \( \mathbb{C} \times \mathbb{C} \) has a Siegel factor. By Bilu-Tichy’s criterion there exists \( \{ \overline{\tau}, \overline{\tau} \} \subset \text{Aut}(\mathbb{C}) \) such that \( \overline{f}, \overline{g} \) admit one of the following factorizations in \( \text{End}(\mathbb{C}, \circ) \):

(i) \( \overline{f} = \epsilon \circ z^m \circ \overline{\tau}, \quad \overline{g} = \epsilon \circ z^r \circ \overline{p}(z)^m \circ \overline{\tau} \).

Let \( i_1 \) be an \( \overline{\tau} \)-lifting of \( i_1^\dagger \) and \( i_2 \) a \( z^m \)-lifting of \( i_1 \). By Proposition 3.8 and an induction argument, \( j_1^{-1} \) is an \( \overline{\tau} \)-lifting of \( i_2 \), and then \( f = \epsilon \circ f_1 \circ \epsilon \) is a relation in \( \text{End}(E, \circ) \) where \( \epsilon, f_1 \) and \( \epsilon \) are obtained by the following commutative diagram:

\[
\begin{array}{cccccc}
\mathbb{C} & \xrightarrow{\tau} & \mathbb{C} & \xrightarrow{z^m} & \mathbb{C} & \xrightarrow{\tau} & \mathbb{C} \\
\downarrow{j_1^{-1}} & & \downarrow{i_2} & & \downarrow{i_1} & & \downarrow{i_1^{-1}} \\
\mathbb{E} & \xrightarrow{\epsilon} & \mathbb{E} & \xrightarrow{f_1} & \mathbb{E} & & \mathbb{E} \\
\end{array}
\]

Similarly if \( i'_2 \) is a \( z^r \circ \overline{p}(z)^m \)-lifting of \( i_1 \), then \( g = \epsilon \circ g_1 \circ \epsilon \) is also a relation in \( \text{End}(E, \circ) \) according to the following commutative diagram:

\[
\begin{array}{cccccc}
\mathbb{C} & \xrightarrow{\tau} & \mathbb{C} & \xrightarrow{z^r \circ \overline{p}(z)^m} & \mathbb{C} & \xrightarrow{\tau} & \mathbb{C} \\
\downarrow{j_2^{-1}} & & \downarrow{i'_2} & & \downarrow{i_1} & & \downarrow{i_1^{-1}} \\
\mathbb{E} & \xrightarrow{\epsilon} & \mathbb{E} & \xrightarrow{g_1} & \mathbb{E} & & \mathbb{E} \\
\end{array}
\]
Write $p=i_1(0), r=i_2(0)$ and $q=i'_2(0)$. The map $f_1$ is totally ramified over $p$ with $r$ above, and $(g_1)_p \equiv r(q) \mod m$. Choosing suitable $\iota_i$ in $\text{Aut}(E)$ and substituting

\begin{align}
\epsilon &\mapsto \epsilon \circ \iota_1^{-1}, \\
\xi &\mapsto \xi \circ \iota_2,
\end{align}

we may assume that $p=r=q=0$, and this leads to the desired assertion.

(ii) $f=\varpi z^2 \circ \iota, \quad g=\varpi (z^2+1) p(z)^2 \circ \iota$.

By arguments similar to that in the proof of the previous case we obtain the relations $f=\varpi \circ f_1 \circ \iota$ and $g=\varpi \circ g_1 \circ \iota$ in $\langle 0 \rangle$ in which $f_1$ is totally ramified over $p$ and $(g_1)_p \equiv (q)+(r) \mod 2$ for some distinct points $q, r$ in $\mathbb{E}$. Choosing suitable $\iota_i$ in $\text{Aut}(E)$ and substituting as in (6.1), we may assume that $p=q=0, r=a$, and this implies our desired assertion.

(iii) $f=\varpi T_m \circ \iota, \quad g=\varpi T_n \circ \iota$ with $(m, n)=1$.

By arguments similar to that in the proof of case (i) we may obtain the relations $f=\varpi \circ f_1 \circ \iota$ and $g=\varpi \circ g_1 \circ \iota$ in $\langle 0 \rangle$ where $f_1, g_1$ are both unramified outside $\{p, q\}$ for some distinct points $p, q$ in $\mathbb{E}$ and their monodromies are Chebyshev representation. By Proposition 27 after substituting as in (6.1) for suitable $\iota_i$ chosen from $\text{Aut}(E)$ we will have $f_1=T_m, n$ and $g_1=T_n, nt$ as desired.

(iv) $f=\varpi T_m \circ \iota, \quad g=\varpi - T_m \circ \iota$ with $(m, n)>1$.

We may apply arguments similar to that in the proof of Case (iii).

(v) $f=\varpi (z^2-1)^3 \circ \iota, \quad g=\varpi (3z^4-4z^3) \circ \iota$.

We first notice that $(z^2-1)^3$ takes $-1$ and $0$ as critical values, $0$ over $0$ and $0$ over $-1$ with ramification index $e_{\pm 1}=3$ and $e_0=2$. Moreover $3z^4-4z^3$ takes also $-1$ and $0$ as critical values, $0$ over $0$ and $1$ over $-1$ with $e_0=3$ and $e_1=2$. By arguments similar to those in the proof of Case (i) we obtain the relations $f=\varpi \circ f_1 \circ \iota, g=\varpi \circ g_1 \circ \iota$ in $\langle 0 \rangle$, where $f_1$ admits two points $q, r$ ramified over some point $p$ with $e_q=e_r=3$ and $g_1$ admits a point $s$ ramified over $p$ with $e_s=3$. Making a replacement as in (6.1) for well-chosen $\iota_i$ in $\text{Aut}(E)$ we may assume that $p=s=0, q=-r$, which gives the desired $f_1$ and $g_1$. The algebraic relation is given by the coincidence of another critical value of $f_1$ and $g_1$.

In Case (i) if $g_1$ is totally ramified with $m \geq 2$, then one checks readily that $g_1$ is ramified over 0. After modifying $\epsilon$ we can assume $\{f_1, g_1\} = \{z^m, z^l\}$.

7. A result on heights

In this section we shall prove Theorem 7.2 by comparing the logarithmic naive height and Call-Silverman’s canonical height. The key ingredient of the proof is a recent theorem of M. Baker [2].

Given a global field $E$ we write $M_E$ for the set of normalized absolute values. Because the Picard group of $\mathbb{P}^1$ is $\mathbb{Z}$, it is clear that for any $\iota \in \text{Aut}(\mathbb{P}^1)$ there exists a positive constant $c$ such that for all $x$ in $\mathbb{P}^1(E)$ we have $|h(\iota(x)) - h(x)| \leq c$.

Given $f \in \text{End}(\mathbb{P}^1)$ that is defined over $E$ the canonical height $h_f(z)$ satisfies that $\hat{h}_f(f^k(z)) = (\deg f)^k \hat{h}_f(z), \ |h(z) - \hat{h}_f(z)|$ is uniformly bounded and in case $E$ is a number field, then $z$ is preperiodic if and only if $\hat{h}_f(z) = 0$. 


Let $E$ be a function field. We call $g \in E(x)$ isotrivial if there is a finite extension $E'$ of $E$ and $\iota \in \text{Aut}_{E'}(\mathbb{P})$ such that $\iota \circ g \circ \iota^{-1}$ is defined over the field of constants.

**Theorem 7.1** (M. Baker). If $E$ is a function field and if $f \in E(\mathbb{P}) \setminus \text{Aut}_E(\mathbb{P})$ is nonisotrivial, then a point $z \in \mathbb{P}(\overline{E})$ is preperiodic if and only if $h_f(z) = 0$.

This theorem is crucial for the proof of the following.

**Theorem 7.2.** Let $\{f, g\} \subset \mathbb{C}(z)$ and let $\{x_0, y_0\} \subset \mathbb{P}$. If $\mathcal{O}_{f \times g}(x_0, y_0)$ has infinitely many points on the diagonal of $\mathbb{P} \times \mathbb{P}$, then $\deg f = \deg g$.

In [8] p. 478 the authors announced that they can prove Theorem 7.2 for polynomials via Benedetto’s theorem together with many other results from polynomial dynamics. Based on some idea of Ghioca-Tucker-Zieve we invoke only Baker’s theorem to prove the above theorem by induction on the transcendental degree of a field of definition of $f, g, x_0, y_0$ over $\mathbb{Q}$. We start with

**Lemma 7.3.** Let $k$ be a number field, $\{f, g\} \subset k(\mathbb{P})$ and $\{x_0, y_0\} \subset \mathbb{P}(k)$. If the orbit $\mathcal{O}_{f \times g}(x_0, y_0)$ has infinitely many points on the diagonal, then $\deg f = \deg g$.

**Proof.** Otherwise we assume that $\deg f < \deg g$ and that there exists $x \in k$ for which $\mathcal{O}_{f \times g}(x, x)$ has infinitely many points on the diagonal. Note that $x$ is not a preperiodic point of $g$, as otherwise $\mathcal{O}_{f \times g}(x, x)$ has at most finitely many points on the diagonal. This leads to $\hat{h}_g(x) > 0$. By properties of heights we have

$$h(g^m(x)) \gg_m \deg m \cdot g.$$  

If $f \notin \text{Aut}_k(\mathbb{P})$, then

$$h(f^m(x)) \ll_m \deg m \cdot f,$$

and if $f$ is in $\text{Aut}_k(\mathbb{P})$, then

$$h(f^m(x)) \ll_m m.$$

By comparing the heights of $f^m(x)$ and $g^m(x)$ we conclude that there are only finitely many $m$ for which $f^m(x) = g^m(x)$. This contradicts our assumption. \qed

To prove Theorem 7.2 we use Lemma 7.3 and the technique of specialization.

**Proof of Theorem 7.2**. For the same reason as in the proof of Lemma 7.3 we may assume $x_0 = y_0 = x$, $\deg f < \deg g$ and $x$ is preperiodic for neither $f$ nor $g$. Objects $f, g$ and $x$ are all defined over a field $k$ of finite type over $\mathbb{Q}$, and we continue with the proof by induction on $\text{tr.deg}(k/\mathbb{Q})$. If $\text{tr.deg}(k/\mathbb{Q}) = 0$, then it reduces to Lemma 7.3. Let $s$ be a positive integer greater such that the claim holds as long as $\text{tr.deg}(K/\mathbb{Q}) \leq s - 1$. Then we will prove it for $\text{tr.deg}(K/\mathbb{Q}) = s$. Choose a subfield $k'$ of $k$ such that $\text{tr.deg}(k/k') = 1$ and then $k$ is the function field of a curve $X$ defined over $k'$. Now we restrict our attention to $k \times k'\overline{K}/\overline{K}$ instead of $k'$. If $g$ is not isotrivial, then we also have $\hat{h}_g(x) > 0$ by Baker’s theorem, and the argument in the proof of Lemma 7.3 still works. Now we assume $g$ is isotrivial. After a conjugation by a linear fractional transformation we may assume $g$ is defined over $\overline{K}$. Now we fall into one of the following two cases:

**Case (i).** $x \in \overline{K}$. We choose $\alpha$ in $X(\overline{K})$ at which $f$ has good reduction and consider the reduction triple $(f_\alpha, g_\alpha = g, x_\alpha = x)$. By assumption $x$ is not preperiodic for $g$ and therefore $x_\alpha$ is not preperiodic for $g_\alpha$. This means that $\mathcal{O}_{f_\alpha \times g_\alpha}(x_\alpha, x_\alpha)$ has infinitely many points on the diagonal, and we are done by the induction assumption.
Case (ii). \( x \notin \bar{\mathbb{F}} \). We will give two alternative arguments. For the first proof we notice that \( x \) is a function of positive degree \( d \) on \( X(\bar{\mathbb{F}}) \) and therefore \( g^m(x) \) is a function of degree \( d \deg m \) on \( X \). Moreover by induction it follows easily that there exists a natural number \( e \) such that for all positive integers \( m \) the function \( f^m(x) \) is of degree at most \( d \deg m f + em \deg f \). We obtain a contradiction by comparing the degrees of \( f^m(x) \) and of \( g^m(x) \). For the second proof we notice that \( g \) is a function in \( \bar{\mathbb{F}}(z) \) and there exists \( q \) in \( \bar{\mathbb{F}} \) such that \( q \) is not preperiodic for \( g \). Let \( \alpha \) be a point in \( X(\bar{\mathbb{F}}) \) for which \( x_{\alpha} \) equals \( q \). We do the reduction at \( \alpha \) and then we complete the proof by the induction assumption. \( \square \)

8. Proof of Theorem 1.1

The comparison of rigidity with speciality of monoid factorizations is implicitly one major originality of \( \mathcal{X} \) and \( \mathcal{B} \), where the authors used the rigidity (cf.Ritt \( \mathcal{R} \)) and the speciality (cf.Bilu-Tichy \( \mathcal{B} \)) of factorizations of \( (\text{End}(\mathbb{C}), \circ) \) to study the dynamics of polynomials. We have obtained the rigidity of factorizations of \( (\text{End}(\mathbb{E}), \circ) \) in Theorem 5.1 and Proposition 5.5 (based on a joint work with Ng), as well as the corresponding speciality result in Theorem 6.2. The former relies on action of fundamental groups, while the latter is governed by finiteness of rational points. In this section we shall adopt the strategy of Ghioca-Tucker-Zieve and work on \( (\text{End}(\mathbb{E}), \circ) \). One more difficulty in carrying their method in our context is the management of elliptic rational functions.

**Proposition 8.1.** If at least one of \( \{ f, g \} \subset \text{End}(\mathbb{E}) \) is not totally ramified, then the equation \( \epsilon \circ f = g \circ \epsilon \) has only finitely many solutions \( \{ \epsilon, \epsilon \} \subset \text{Aut}(\mathbb{E}) \).

**Proof.** We assume that \( f \) is not totally ramified and then the degree of \( |\mathcal{D}_f| \) and of \( \mathcal{D}_f \) are at least two. If \( \{ \epsilon, \epsilon \} \subset \text{Aut}(\mathbb{E}) \) gives a solution to \( \epsilon \circ f = g \circ \epsilon \), then \( \epsilon \) (resp.\( \epsilon \)) induces a bijection from \( \mathcal{D}_f \) to \( \mathcal{D}_g \) (resp. from \( |\mathcal{D}_f| \) to \( |\mathcal{D}_g| \)). The natural map

\[
\{(\epsilon, \epsilon) \mid \epsilon \circ f = g \circ \epsilon \} \to \text{Hom}(\mathcal{D}_f, \mathcal{D}_g) \times \text{Hom}(|\mathcal{D}_f|, |\mathcal{D}_g|)
\]

is injective since the only element in \( \text{Aut}(\mathbb{E}) \) that fixes at least two points must be the identity map. This leads to the desired assertion. \( \square \)

Finite Blaschke products \( f, g \) are called *commensurable* in \( (\text{End}(\mathbb{E}), \circ) \) if for any positive integer \( m \) there exist \( \{ h_1, h_2 \} \subset \text{End}(\mathbb{E}) \) and positive integer \( n \) such that

\[
f^n = g^m \circ h_1, \quad g^n = f^m \circ h_2.
\]

**Lemma 8.2.** Let \( f \in \text{End}(\mathbb{E}) \setminus \text{Aut}(\mathbb{E}) \) and \( \iota \in \text{Aut}(\mathbb{E}) \). If there are infinitely many \( n \) such that \( f^n = (f \circ \iota)^n \circ \iota_n \) for some \( \iota_n \in \text{Aut}(\mathbb{E}) \), then one of the following assertions is satisfied:

(i) There exists \( k \in \mathbb{N} \) for which \( f^k = (f \circ \iota)^k \).

(ii) There exist \( \{ \mu, \rho \} \subset \mathbb{T} \) and \( \iota \in \text{Aut}(\mathbb{E}) \) such that \( f = \epsilon \circ \mu z^d \circ \epsilon^{-1} \) and \( \iota = \epsilon \circ \rho z \circ \epsilon^{-1} \).

**Proof.** By Corollary 5.6 applied to \( f^n = (f \circ \iota)^n \circ \iota_n \), there exist \( \{ \epsilon_n, \overline{\epsilon_n} \} \subset \text{Aut}(\mathbb{E}) \) such that \( f \circ \iota \circ \epsilon_n = \epsilon_n \circ f \) and \( f \circ \iota \circ \epsilon_n = \overline{\epsilon_n} \circ f^2 \).

**Case (i).** \( f \) is not totally ramified. By Proposition 8.1 there exists \( n < m \) such that \( \iota_n = \iota_m \). This gives \( f^m = (f \circ \iota)^m \circ \iota_n = (f \circ \iota)^m \circ \iota_n = (f \circ \iota)^m \circ \iota_n = (f \circ \iota)^m \circ f^m \) and therefore \( f^{m-n} = (f \circ \iota)^{m-n} \).

**Case (ii).** \( f^2 \text{ (equivalently } f \circ f \text{) is not totally ramified. A similar argument works.} \)
Case (iii). $f, f^2$ and $f \circ \iota \circ f$ are all totally ramified. Write $q = |D_f|$ and $p = D_f$. Because $f^2$ (resp. $f \circ f$) is totally ramified we have $q = p$ (resp. $p(p) = p$). Consequently there exist $\{\mu, \rho\} \subset \mathbb{T}$ such that $f = \iota_p \circ \mu \circ z^d \circ p$ and $\iota = \iota_p \circ \rho \circ z^d \circ p$. \hfill \qed

We first prove

**Proposition 8.3.** If $\{f, g\} \subset \text{End}(E) \setminus \text{Aut}(E)$ are commensurable, then either $f$ and $g$ have common iterates or there exist $\iota \in \text{Aut}(E)$ and $\mu \in \mathbb{T}$ such that

$$\iota \circ f \circ \iota^{-1} = \mu z^r, \quad \iota \circ g \circ \iota^{-1} = \mu z^s$$

where $r = \deg f$ and $s = \deg g$.

**Proof.** By the commensurability assumption, for $m \in \mathbb{N}$ there exist $n \in \mathbb{N}$ and $\{h_1, h_2\} \subset \text{End}(E)$ such that

$$f^n = g^m \circ h_1, \quad g^n = f^m \circ h_2.$$  

Case (i). There exist $\{k, l\} \subset \mathbb{N}$ such that $r^k = s^l$. For any $m \in \mathbb{N}$ we choose $n_m \in \mathbb{N}$ and $\varepsilon_m \in \text{End}(E)$ for which $f^{m} \circ \varepsilon_m \circ g = g^m$ or equivalently $f^{m} \circ \varepsilon_m \circ g = g^{m} \circ g^{m} - m$. The condition $r^k = s^l$ leads to $\deg f^{m} = \deg g^{m}$, and then Proposition 5.5 implies that there exists $t_m \in \text{End}(E)$ for which $g^{m} = f^{m} \circ t_m$. Consequently for all positive integers $m$ we have $(f^{k}m) = (f^{k}t_{m})$ and this reduces to Lemma 8.2.

Case (ii). There exists no $\iota \in \text{Aut}(E)$ for which $\iota \circ g \circ \iota^{-1} = z^s$. For any $m \in \mathbb{N}$ we denote by $n_m$ the minimal integer such that $g^{m} = f^{m} \circ \varepsilon_m$ for some $\varepsilon_m \in \text{End}(E)$. The minimality of $n_m$ forces that there exists no $t \in \text{End}(E)$ for which $\varepsilon_m = \text{deg} g$, and therefore by Corollary 5.19, there exist positive integers $m < p$ such that $\deg \varepsilon_m = \deg \varepsilon_p$. This leads to $s^m - n_m = r^p - m$, which reduces the problem to the previous case.

Case (iii). There exists $\iota \in \text{Aut}(E)$ such that $\iota \circ g \circ \iota^{-1} = z^s$. For $m \in \mathbb{N}$ there exist $\varepsilon_m \in \text{End}(E)$ and $n_m \in \mathbb{N}$ such that $f^{m} \circ \varepsilon_m = g^{m}$ or equivalently

$$f^{m} \circ \varepsilon_m \circ \iota^{-1} = \iota^{-1} \circ \varepsilon_m \circ \iota^{-1} = \iota^{-1} \circ \varepsilon_m \circ \iota^{-1} \circ \varepsilon_m^{-1} \circ \iota^{-1} \circ \varepsilon_m^{-1} \circ \iota^{-1}.$$

Proposition 5.5 implies that $f \sim z^m$, and then Corollary 5.7 applies. \hfill \qed

We then prove

**Proposition 8.4.** If $\{f, g\} \subset \text{End}(E) \setminus \text{Aut}(E)$ are noncommensurable and if for all $\{m, n\} \subset \mathbb{N}$ the curve $\mathbb{P}^{1} \times f^{m}, g^{n} \mathbb{P}^{1}$ admits a Faltings factor, then there exist $\iota \in \text{Aut}(E)$ and $\mu \in \mathbb{T}$ such that

$$\iota \circ f \circ \iota^{-1} = \mu z^r, \quad \iota \circ g \circ \iota^{-1} = \mu z^s$$

where $r = \deg f$ and $s = \deg g$.

**Proof.** By the assumption that $f$ and $g$ are noncommensurable there exist $t \in \mathbb{N}$ such that for any $n \in \mathbb{N}$ and for any $p \in \text{End}(E)$,

$$g^n \neq f^t \circ h.$$  

Given $\{i, j\} \subset \mathbb{N}$, by the existence of the Faltings factor of $\mathbb{P}^{1} \times (f^{i}), g^{j} \mathbb{P}^{1}$ and by Theorem 6.2 there exist $\{a_{ij}, b_{ij}, c_{ij}\} \subset \text{End}(E)$ and $\{e_{ij}, e_{ij}\} \subset \text{End}(E)$ such that

$$(f^{i})^{j} = a_{ij} \circ b_{ij} \circ e_{ij}, \quad g^{j} = a_{ij} \circ c_{ij} \circ e_{ij},$$

where the set $\{b_{ij}, c_{ij}\}$ is described in Theorem 6.2. We write $S = \{\text{deg} a_{ij} : (i, j) \in \mathbb{N} \times \mathbb{N}\}$ and consider the following two cases.
Case (i). The cardinality of \( S \) is infinite. Given any \( h \in \text{End}(\mathbb{E}) \) and any pair \( \{i,j\} \subset \mathbb{N} \) we have

\[
(8.2) \quad a_{ij} \neq f^i \circ h.
\]

Otherwise \( g^j = a_{ij} \circ c_{ij} \circ \epsilon_{ij} = f^i \circ (h \circ c_{ij} \circ \epsilon_{ij}) \), a contradiction to (8.1). Because the cardinality of \( S \) is infinite, Corollary 5.19 and (8.2) applied to \( a_{ij} \circ (b_{ij} \circ \epsilon_{ij}) = (f^i)^j \) shows that \( \circ f^i \circ \sigma^{-1} = z^r \) for some \( \sigma \in \text{Aut}(\mathbb{E}) \). In particular \( f^i \) is totally ramified, and this together with Corollary 5.7 leads to the existence of \( \sigma \in \text{Aut}(\mathbb{E}) \) for which \( \sigma \circ f \circ \sigma^{-1} = z^r \). Neither the hypothesis nor the conclusion is affected under

\[
f \mapsto \sigma \circ f \circ \sigma^{-1}, \quad g \mapsto \sigma \circ g \circ \sigma^{-1}.
\]

We may assume \( f(z) = z^r \) and then \( b_{ij} \), as a factor of \( z^{rti} \), is totally ramified. Henceforth we always assume that \( i \) is so large compared to \( j \) that \( \deg b_{ij} > \deg c_{ij} \), which forces \( \{b_{ij}, c_{ij}\} \) to fall into Case (i) of Theorem 6.2 and \( c_{ij} \) to be totally ramified. By the remark after Theorem 6.2 we assume that \( \{b_{ij}, c_{ij}\} = \{z^m, z^r\} \), namely,

\[
(8.3) \quad (z^{tr})^i = a_{ij} \circ b_{ij} \circ \epsilon_{ij}, \quad g^j = a_{ij} \circ c_{ij} \circ \epsilon_{ij}
\]

with \( b_{ij} = z^m, c_{ij} = z^r \) and \( \{\epsilon_{ij}, \epsilon_{ij}\} \subset \text{Aut}(\mathbb{E}) \). It is clear that for nonlinear \( a \) and \( b \), \( a \circ b \) is totally ramified if and only if \( a \) and \( b \) are and \( |\mathcal{D}_a| = |\mathcal{D}_b| \). Our factorization of \( (z^{tr})^i \) implies that \( a_{ij} \) is totally ramified and \( |\mathcal{D}_{a_{ij}}| = |\mathcal{D}_{b_{ij}}| \). This together with \( b_{ij} = z^m \) and \( c_{ij} = z^r \) leads to \( |\mathcal{D}_{a_{ij}}| = |\mathcal{D}_{c_{ij}}| \), and therefore \( g^j \), which equals \( a_{ij} \circ c_{ij} \circ \epsilon_{ij} \), is also totally ramified. By Corollary 5.7 applied to \( g^j \) there exists \( \tau \in \text{Aut}(\mathbb{E}) \) such that \( \tau \circ g \circ \tau^{-1} = z^s \). It is clear from (8.3) that \( \mathcal{D}_{g^j} = \mathcal{D}_{a_{ij}} = \mathcal{D}_{z^s} = 0 \) and therefore \( \mathcal{D}_g = 0 \). This together with \( \tau \circ g \circ \tau^{-1} = z^s \) implies that \( g(z) = \mu z^s \) for some \( \mu \in \mathbb{T} \).

Case (ii). The cardinality of \( S \) is finite. If \( (r,s) = 1 \), then we always have \( \deg a_{ij} = 1 \). We only consider the case that \( i \) and \( j \) are at least three. By Corollary 5.8 neither \( f^{ti} \) nor \( g^j \) is elliptic, and therefore \( \{b_{ij}, c_{ij}\} \) falls into Case (i) of Theorem 6.2. The one of \( \{b_{ij}, c_{ij}\} \) with smaller degree must be totally ramified, and so is \( \{f^{ti}, g^j\} \) as \( \deg a_{ij} = 1 \). Choose either \( i \) or \( j \) to be arbitrarily large; we deduce that \( f^{3t} \) and \( g^3 \) are both totally ramified. By Corollary 5.7 there exist \( \{\epsilon, \epsilon\} \subset \text{Aut}(\mathbb{E}) \) such that \( \epsilon \circ f \circ \epsilon^{-1} = z^r \) and \( \epsilon \circ g \circ \epsilon^{-1} = z^s \). It remains to show that \( \mathcal{D}_f = \mathcal{D}_g \). Indeed by the remark made at the end of Section 6 we have that \( \mathcal{D}_{b_{ij}} = \mathcal{D}_{c_{ij}} = 0 \) and therefore \( \mathcal{D}_f = \mathcal{D}_g = a_{ij}(0) \).

If \( (r,s) \neq 1 \), then by the finiteness of \( |S| \) we have \( \min \{\deg b_{ij}, \deg c_{ij}\} \to \infty \) as \( \min \{i, j\} \to \infty \), and hence for large \( i \) and \( j \) the pair \( \{f^{ti}, g^j\} \) falls into Case (iv) of Theorem 6.2. If we choose sufficiently large positive integers \( p, n \) and \( m \) with \( n+3 \leq m \) such that \( \deg a_{p,n} = \deg a_{p,m} \), then

\[
g^n = a_{p,n} \circ c_{p,n} \circ \epsilon_{p,n}, \quad g^m = a_{p,m} \circ c_{p,m} \circ \epsilon_{p,m}
\]

where \( c_{p,n}, c_{p,m} \) are elliptic. This gives

\[
a_{p,n} \circ (c_{p,n} \circ \epsilon_{p,n} \circ g^{m-n}) = a_{p,m} \circ (c_{p,m} \circ \epsilon_{p,m}).
\]

Corollary 5.6 gives \( c_{p,n} \circ \epsilon_{p,n} \circ g^{m-n} \sim c_{p,m} \), and then Corollary 5.9 implies that \( g^{m-n} \) is elliptic, a contradiction to Corollary 5.8. \qed
Combining previous results, we readily prove the main theorem.

**Proof of Theorem 1.1.** The infiniteness of $O_f(x) \cap O_g(y)$ implies that for all positive integers $m, n$ there are infinitely many rational points on $\mathbb{P}^1 \times f^n, g^m \mathbb{P}^1$ over the absolute field $k$ generated by all coefficients of $f, g$ and $x, y$. Indeed by assumption for $i \geq 1$ there exist pairwise distinct points $p_i, q_i \in \mathbb{P}^1$ and $\{n_i, m_i\} \subset \mathbb{N}$ such that

$$f^{n_i}(x) = p_i, \quad g^{m_i}(y) = q_i.$$ 

It is clear that $n_i$ (resp. $m_i$) are also pairwise distinct and therefore tend to infinity as $i$ goes to infinity. Therefore for $i$ sufficiently large, $(f^{n_i}(x), g^{m_i}(y))$ are $k$-rational points of $\mathbb{P}^1 \times f^n, g^m \mathbb{P}^1$. These points are pairwise distinct, as otherwise $x$ would be preperiodic for $f$, which contradicts the infiniteness assumption.

By Faltings’ theorem the curve $\mathbb{P}^1 \times f^n, g^m \mathbb{P}^1$ has a Faltings factor. If $f$ and $g$ have no common iterate, then by Proposition 8.3 and Proposition 8.4 we may assume that $f = z^r, g = \mu z^s$ with $\mu \in \mathbb{T}$. This case is already discussed in [9]. □

It is crucial to require that $f, g \notin \text{Aut}(\mathbb{E})$ in Theorem 1.1. For an example we consider $\mathbb{H}$ instead of $\mathbb{E}$ and simply take $f(z) = z+1, g(z) = 2z$ and $x = y = 1$.

**Acknowledgement**

The author thanks the referees for helpful suggestions.

**References**

[1] Lars V. Ahlfors and Leo Sario, *Riemann surfaces*, Princeton Mathematical Series, No. 26, Princeton University Press, Princeton, N.J., 1960. MR0114911 (22 #5729)

[2] Matthew Baker, *A finiteness theorem for canonical heights attached to rational maps over function fields*, J. Reine Angew. Math. 626 (2009), 205–233, DOI 10.1515/CRELLE.2009.008. MR2492995 (2011c:14075)

[3] Yuri F. Bilu and Robert F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. 95 (2000), no. 3, 261–288. MR1793164 (2001i:11031)

[4] Gregory S. Call and Joseph H. Silverman, *Canonical heights on varieties with morphisms*, Compositio Math. 89 (1993), no. 2, 163–205. MR1255693 (95d:11077)

[5] A. B. Bogatyrev, *Chebyshev representation of rational functions* (Russian, with Russian summary), Mat. Sb. 201 (2010), no. 11, 19–40, DOI 10.1070/SM2010v201n11ABEH004123; English transl., Sb. Math. 201 (2010), no. 11-12, 1579–1598. MR2768552 (2011k:30047)

[6] K. Chandrasekharan, *Elliptic functions*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 281, Springer-Verlag, Berlin, 1985. MR080396 (87e:11058)

[7] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörperrn* (German), Invent. Math. 73 (1983), no. 3, 349–366, DOI 10.1007/BF01388432. MR718935 (85g:11026a)

[8] Dragos Ghioca, Thomas J. Tucker, and Michael E. Zieve, *Intersections of polynomials orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math. 171 (2008), no. 2, 463–483, DOI 10.1007/s00222-007-0087-5. MR2367026 (2008k:37099)

[9] Dragos Ghioca, Thomas J. Tucker, and Michael E. Zieve, *Linear relations between polynomial orbits*, Duke Math. J. 161 (2012), no. 7, 1379–1410, DOI 10.1215/00127094-1598098. MR2922378

[10] M. D. Lutovac, D. V. Toci, and B. L. Evans, *Filter Design for Signal Processing using MATLAB and Mathematica*, Prentice Hall, New Jersey, 2001.

[11] Tuen Wai Ng and Ming-Xi Wang, *Ritt’s theory on the unit disk*, Forum Math. 25 (2013), no. 4, 821–851, DOI 10.1515/form.2011.136. MR3089751

[12] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), no. 1, 51–66, DOI 10.2307/1988911. MR1501189
[13] I. R. Shafarevich (ed.), *Algebraic geometry. I: Algebraic curves. Algebraic manifolds and schemes*, Encyclopaedia of Mathematical Sciences, vol. 23, Springer-Verlag, Berlin, 1994. A translation of *Current problems in mathematics. Fundamental directions, Vol. 23 (Russian)*, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1988; Translation by D. Coray and V. N. Shokurov. MR1287418 (95b:14001)

[14] Carl L. Siegel, *Über einige Anwendungen diophantischer Approximationen* [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1] (German), On some applications of Diophantine approximations, Quad./Monogr., vol. 2, Ed. Norm., Pisa, 2014, pp. 81–138. MR3330350

[15] M. X. Wang, http://hub.hku.hk/handle/123456789/51854, MPhil Thesis (2008).

[16] M. X. Wang, *Rational points and transcendental points*, PhD thesis (2011).

[17] M. E. Zieve and P. Müller, *On Ritt’s polynomial decomposition theorems*, arXiv:0807.3578.

[18] E. I. Zolotarev, *Application of elliptic functions to the question of the functions least and most deviating from zero*, 1877.

Department of Mathematics, University of Salzburg, Hellbrunnerstr. 34/I, 5020 Salzburg, Austria

E-mail address: mingxi.waeng@gmail.com