Math. Proc. Camb. Phil. Soc. (2024), **177**, 149–165
doi:10.1017/S0305004124000173
First published online 19 September 2024

Multiplicative dependence of rational values modulo approximate finitely generated groups

BY ATTILA BÉRCZES
Institute of Mathematics, University of Debrecen, H-4010 *Debrecen, P.O. BOX* 12*, Hungary*
e-mail: berczesa@science.unideb.hu

YANN BUGEAUD
Institut de Recherche Mathématique Avancée, U.M.R. 7501*, Université de Strasbourg et C.N.R.S.,* 7*, rue René Descartes,* 67084 *Strasbourg, France; Institut Universitaire de France*
e-mail: yann.bugeaud@math.unistra.fr

KÁLMÁN GYŐRY
Institute of Mathematics, University of Debrecen, H-4010 *Debrecen, P.O. Box* 12*, Hungary*
e-mail: gyory@science.unideb.hu

JORGE MELLO
Department of Mathematics and Statistics, Oakland University, 48307 *Michigan, United States*
e-mail: jorgedemellojr@oakland.edu

ALINA OSTAFE
School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052*, Australia*
e-mail: alina.ostafe@unsw.edu.au

AND MIN SHA
School of Mathematical Sciences, South China Normal University, Guangzhou 510631*, China*
e-mail: min.sha@m.scnu.edu.cn

(*Received* 17 *August* 2022*; revised* 26 *November* 2023*; accepted* 22 *April* 2024)

Abstract

In this paper, we establish some finiteness results about the multiplicative dependence of rational values modulo sets which are 'close' (with respect to the Weil height) to division groups of finitely generated multiplicative groups of a number field K. For example, we show that under some conditions on rational functions $f_1, \dots, f_n \in K(X)$, there are only finitely many elements $\alpha \in K$ such that $f_1(\alpha), \dots, f_n(\alpha)$ are multiplicatively dependent modulo such sets.

2020 Mathematics Subject Classification: 11N25 (Primary); 11R04 (Secondary)

© The Author(s), 2024. Published by Cambridge University Press on behalf of Cambridge Philosophical Society.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

1. *Introduction*

1.1. Motivation

Given non-zero complex numbers $\alpha_1, \dots, \alpha_n \in \mathbb{C}^*$, we say that they are *multiplicatively dependent* if there exist integers $k_1, \dots, k_n \in \mathbb{Z}$, not all zero, such that

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} = 1;$$

and we say that they are *multiplicatively dependent modulo G*, where G is a subset of $\mathbb{C}^*$, if there exist integers $k_1, \dots, k_n \in \mathbb{Z}$, not all zero, such that

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} \in G.$$

Multiplicative dependence of algebraic numbers has been studied for a long time and still very actively; see, for instance, [**4**, **5**, **12**, **14**, **19**, **22**, **27**, **28**, **31**, **35**, **41**] and the references therein. The authors in [**28**] have studied the multiplicative dependenc of elements in an orbit of an algebraic dynamical system, and recently in [**9**] this has been extended to the more general setting of multiplicative dependence modulo a finitely generated multiplicative group.

In this paper, we want to study multiplicative dependence among values of rational functions modulo sets which can be roughly described as *approximate division groups* of finitely generated groups Γ, denoted by $\Gamma_\varepsilon^{\mathrm{div}}$ (which is defined in the next section), that is, sets which are not far with respect to the Weil height from the division group of a finitely generated multiplicative group of a number field.

The motivation also partly comes from the study of points on subvarieties of tori. Let $\mathbb{G}_{\mathrm{m}}$ be the multiplicative algebraic group over the complex numbers $\mathbb{C}$, that is $\mathbb{G}_{\mathrm{m}} = \mathbb{C}^*$ endowed with the multiplicative group law. Intersection of varieties in ${\mathbb{G}_{\mathrm{m}}}^n$ with sets of the type $\Gamma_\varepsilon^{\mathrm{div}}$ falls within two conjectures, the *Mordell–Lang conjecture* on intersection of varieties with finitely generated subgroups and the *Bogomolov conjecture* which is about the discreteness of the set of points of bounded height in a variety. This direction has been extensively studied over several decades, see [**1**, **3**, **8**, **10**, **13**, **16**, **20**, **21**, **23**, **26**, **32**, **33**, **36**, **39**] and references therein, which in particular give precise quantitative results about the intersection of varieties with $\Gamma_\varepsilon^{\mathrm{div}}$.

Here, in some sense, instead of assuming each coordinate of a point is from $\Gamma_\varepsilon^{\mathrm{div}}$, we impose that the coordinates of a point multiplicatively generate an element in $\Gamma_\varepsilon^{\mathrm{div}}$.

1.2. Notation

Throughout the paper, we use the following notation:

(i) K is a number field;
(ii) $\overline{K}$ is an algebraic closure of K;
(iii) S is a finite set of places of K containing all the infinite places;
(iv) O_S is the ring of S-integers of K;
(v) R^* is the unit group of a ring R;
(vi) Γ is a finitely generated subgroup of K^*;
(vii) For $A \subseteq K^*$,

$$A^{\mathrm{div}} := \{\alpha \in \overline{K} : \alpha^m \in A \text{ for some integer } m \geq 1\}.$$

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

For $\varepsilon > 0$,

$$\Gamma_{\varepsilon}^{\mathrm{div}} := \{\alpha\beta : \alpha \in \Gamma^{\mathrm{div}}, \beta \in \overline{K}^* \text{ with } \mathrm{h}(\beta) \leq \varepsilon\}.$$

Here $\mathrm{h}(\cdot)$ stands for the absolute logarithmic Weil height function. The set Γ^{div} is called the division group of Γ.

In addition, let M_K be the set of places of K, M_K^{∞} the set of infinite places of K, and $M_K^0 = M_K \setminus M_K^{\infty}$.

1.3. Main results

In this section we state the main results proved in this paper. Informally, our results can be summarised as follows: given $f_1, f_2, \ldots, f_n \in K[X]$ satisfying some natural conditions (some results hold for rational functions as well), we prove finiteness of the sets of:

- $\alpha \in K$ such that $f_1(\alpha), \ldots, f_n(\alpha)$ are multiplicatively dependent modulo $\Gamma_{\varepsilon}^{\mathrm{div}}$;
- $\alpha \in \Gamma_{\varepsilon}^{\mathrm{div}}$ such that $f_1(\alpha), \ldots, f_n(\alpha)$ are multiplicatively dependent modulo $\Gamma_{\varepsilon}^{\mathrm{div}}$.

We would like to unify these results and have a finiteness result for the set of $\alpha \in K(\Gamma^{\mathrm{div}})$ satisfying the conclusion above, and thus we conclude this section with an open problem in this direction.

We now formally state our results.

THEOREM 1·1. *Let $f_1, f_2, \ldots, f_n \in K[X]$ be pairwise coprime polynomials. Assume that each of them has at least two distinct roots. Then, for every $\varepsilon > 0$ there are only finitely many elements $\alpha \in K$ such that $f_1(\alpha), \ldots, f_n(\alpha)$ are multiplicatively dependent modulo $\Gamma_{\varepsilon}^{div}$.*

We first remark that in Theorem 1·1, since $\alpha \in K$ and the polynomials $f_1, \ldots, f_n$ are in $K[X]$, by Lemma 2·1 below we know that "modulo $\Gamma_{\varepsilon}^{\mathrm{div}}$" can be reduced to modulo a subset of K^* which is somehow "close" to Γ.

We also remark that in Theorem 1·1 the two conditions of the polynomials being "pairwise coprime" and "each of them has at least two distinct roots" somehow cannot be removed. For example, choosing $f_1 = X(X+2)$, $f_2 = (X+1)(X+2)$, and $f_3, \ldots, f_n$ arbitrary, for any $\alpha = 1/(\beta - 1)$ with $\beta \in \Gamma$ and $\beta \neq 1, 1/2$ and $f_3(\alpha) \cdots f_n(\alpha) \neq 0$, we have

$$f_1(\alpha)^{-1} f_2(\alpha)\,(f_3(\alpha) \cdots f_n(\alpha))^0 = \beta \in \Gamma.$$

In addition, choosing pairwise coprime polynomials $f_1, f_2, \ldots, f_n \in K[X]$ with $f_1 = X - a$ for some $a \in K$, for any $\alpha \in \Gamma$ satisfying $f_2(\alpha + a) \cdots f_n(\alpha + a) \neq 0$, we have

$$f_1(\alpha + a)\big(f_2(\alpha + a) \cdots f_n(\alpha + a)\big)^0 = \alpha \in \Gamma.$$

Using Theorem 1·1, we establish the following result, which holds for rational functions. For this, we say that non-zero rational functions $f_1, \ldots, f_n \in K(X)$ are *multiplicatively independent modulo constants* if they are multiplicatively independent modulo K^*, that is, there is no non-zero integer vector $(k_1, \ldots, k_n)$ such that

$$f_1^{k_1} \cdots f_n^{k_n} \in K^*.$$

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

In addition, for any rational function $f \in K(X)$, the numerator and denominator of f are meant to be two polynomials $g, h \in K[X]$, respectively, such that $f = g/h$ and $\gcd(g, h) = 1$.

THEOREM 1·2. *Let $f_1, f_2, \ldots, f_n \in K(X)$ be non-constant rational functions such that they are multiplicatively independent modulo constants. Assume that for each f_i, $i = 1, 2, \ldots, n$, its numerator either has no linear factor or has at least two distinct linear factors over K, and so does its denominator. Assume further that $f_1, f_2, \ldots, f_n$ have distinct linear factors over K (if they have). Then, for every $\varepsilon > 0$ there are only finitely many elements $\alpha \in K$ such that $f_1(\alpha), \ldots, f_n(\alpha)$ are multiplicatively dependent modulo Γ_ε^{div}.*

Remark 1·3. If $f_1, f_2, \ldots, f_n \in K(X)$ in Theorem 1·2 are all monic (that is, both numerator and denominator are monic), then the assumption "they are multiplicatively independent modulo constants" can be replaced by "they are multiplicatively independent".

The following corollary is about multiplicative dependence in orbits of a rational function, which somehow can be viewed as an extension of [9, theorem 1·7]. For a rational function $f \in K(X)$ and a positive integer $n \geq 1$, let $f^{(n)}$ be the nth compositional iterate of f. In addition, for any rational function $f \in K(X)$, if both its numerator and denominator have no linear factor over K, we say that *f has no linear factor*.

COROLLARY 1·4. *Let $f \in K(X)$ be a non-constant rational function satisfying one of the following two conditions*:

(i) $f \in K[X]$, f has at least two distinct roots, and 0 is not a periodic point of f;

(ii) f has no linear factor.

Then, for any $\varepsilon > 0$ and any integer $n \geq 1$, there are only finitely many elements $\alpha \in K$ such that $f^{(m+1)}(\alpha), \ldots, f^{(m+n)}(\alpha)$ are multiplicatively dependent modulo $\Gamma_\varepsilon^{\mathrm{div}}$ for some integer $m \geq 0$.

When $n = 2$ in Theorem 1·1, we can relax the condition of coprimality on the polynomials f_1 and f_2.

We say that $f_1, \ldots, f_n \in \mathbb{C}(X)$ *multiplicatively generate* a rational function g if there exist integers $k_1, \ldots, k_n \in \mathbb{Z}$, not all zero, such that

$$f_1^{k_1} \cdots f_n^{k_n} = g.$$

We have the following result:

THEOREM 1·5. *Let $f_1, f_2 \in K[X]$ be polynomials of degree at least 2, each having at least two distinct roots. Assume that they cannot multiplicatively generate a power of a linear fractional function. Then, for any $\varepsilon > 0$ there are only finitely many elements $\alpha \in K$ such that $f_1(\alpha)$ and $f_2(\alpha)$ are multiplicatively dependent modulo Γ_ε^{div}.*

In Theorem 1·5, the condition related to linear fractional function cannot be removed. See the example below Theorem 1·1. Here, we view non-zero constants as linear fractional functions.

We remark that in Theorem 1·5 we can replace the condition related to linear fractional function with the total number of distinct roots of f_1 and f_2 which are not common roots being at least three.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

We also remark that the results in Theorems 1·1 and 1·5 are both not effective, due to Lemma 2·2.

As a direct consequence of Maurin's theorem [24, théorème 1·2] (see [**11**] for an effective version), if $f_1, f_2, \ldots, f_n \in K(X)$ are such that $X, f_1, \ldots, f_n$ are multiplicatively independent modulo Γ, then the set

$$\left\{\alpha \in \Gamma^{\mathrm{div}} : f_1(\alpha), \ldots, f_n(\alpha) \text{ multiplicatively dependent mod } \Gamma^{\mathrm{div}}\right\} \tag{1·1}$$

is finite (see [30, lemma 3·2] for more details). This is an effective generalisation of Liardet's theorem [21, théorème 1] on division points on curves; see also [8, theorem 2·2] for an effective version of Liardet's result.

We remark that by definition, multiplicative dependence modulo Γ is equivalent to multiplicative dependence modulo Γ^{div}.

Using [25, théorème 1·10], which improves [24, théorème 1·7], we are able to extend this conclusion by enlarging Γ^{div} to $\Gamma_{\varepsilon}^{\mathrm{div}}$ for certain $\varepsilon > 0$ (but in a non-effective manner).

THEOREM 1·6. *Let $f_1, f_2, \ldots, f_n \in K(X)$ be such that $X, f_1, \ldots, f_n$ are multiplicatively independent modulo Γ. Then, there exists a real number $\varepsilon > 0$ for which there are only finitely many elements $\alpha \in \Gamma_{\varepsilon}^{div}$ such that $f_1(\alpha), \ldots, f_n(\alpha)$ are multiplicatively dependent modulo $\Gamma_{\varepsilon}^{div}$.*

We end this section with an open problem. We would like to combine Theorem 1·1 with the finiteness of the set (1·1), and ask the following question:

Problem 1·7. Let $f_1, \ldots, f_n \in K(X)$ be non-zero rational functions. Under what conditions is the following set

$$\left\{\alpha \in K(\Gamma^{\mathrm{div}}) : f_1(\alpha), \ldots, f_n(\alpha) \text{ multiplicatively dependent mod } \Gamma^{\mathrm{div}}\right\} \tag{1·2}$$

finite?

When $\Gamma = \{1\}$, then Γ^{div} is the set of all roots of unity, and $K(\Gamma^{\mathrm{div}})$ is the cyclotomic closure of K. In this case, it has been proven in [28, theorem 4·2] that if $f_1, \ldots, f_n$ do not multiplicatively generate a power of a linear fractional function, then the set (1·2) is finite (in fact, the result holds more generally for the abelian closure of K).

When $n = 1$, Problem 1·7 becomes that for a non-zero rational function $f \in K(X)$, under which condition the set $\{\alpha \in K(\Gamma^{\mathrm{div}}) : f(\alpha) \in \Gamma^{\mathrm{div}}\}$ is finite. This would extend the cyclotomic version of the Hilbert Irreducibility Theorem proved by Dvornicich and Zannier [15, corollary 1] in the case when $\Gamma = \{1\}$. Recall also that a special case of a general conjecture of Rémond (see [37, conjecture 3·4]) asserts that there exists a constant c_Γ such that for any $\alpha \in K(\Gamma^{\mathrm{div}}) \setminus \Gamma^{\mathrm{div}}$, $\mathrm{h}(\alpha) \geq c_\Gamma$ (see [34, conjecture 1·1 (c)], and see [2, theorem 1·3] for a non-trivial example). Clearly, under this conjecture, the finiteness of the set $\{\alpha \in K(\Gamma^{\mathrm{div}}) : f(\alpha) \in \Gamma^{\mathrm{div}}\}$ implies the finiteness of the set $\{\alpha \in K(\Gamma^{\mathrm{div}}) : \mathrm{h}(f(\alpha)) < \varepsilon\}$ for any $\varepsilon < c_\Gamma$.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

2. *Preliminaries*

2.1. On some intersections with approximate groups and algebraic subgroups

We define the set $\mathscr{A}(K, H)$ as the set of nonzero elements in the algebraic number field K of height at most H, that is,

$$\mathscr{A}(K, H) = \left\{\alpha \in K^* : \mathrm{h}(\alpha) \leq H\right\}.$$

We note that by Northcott's Theorem the set $\mathscr{A}(K, H)$ is a finite set.

We need the following result from [29, theorem 2·1].

LEMMA 2·1. *Let* $\{g_1, \ldots, g_r\}$ *be a set of generators of* Γ*, which minimises* $H = \max_{i=1,\ldots,r} h(g_i)$*. Then, for every* $\varepsilon > 0$*, we have*

$$K^* \cap \Gamma_\varepsilon^{div} \subseteq \left\{\beta\eta : (\beta, \eta) \in \Gamma \times \mathscr{A}(K, \varepsilon + rH)\right\}.$$

As usual, for any non-constant rational function $f \in K(X)$, the degree of f is defined to be the maximum of the degrees of its numerator and denominator.

The following result is [9, theorem 1·2 (a)].

LEMMA 2·2. *Let* $f \in K(X)$ *be a rational function of degree* $d \geq 2$*. Assume that* f *is not of the form* $a(X-b)^d$ *or* $a(X-b)^d/(X-c)^d$ *with* $a, b, c \in K$*,* $a(b-c) \neq 0$*, and* $d \in \mathbb{Z}$*. Then, the set* $\{\alpha \in K : f(\alpha) \in \Gamma\}$ *is finite.*

We remark that the result in Lemma 2·2 is not effective, due to the use of the Faltings theorem [**17**] about finiteness of rational points on a curve. See also [29, corollary 2·2] and references therein.

We conclude this section with a result of Maurin [25, théorème 1·10], which we present in our setting of parametric curves by noticing [25, remarque 1·3].

For this we introduce the following notation: we define $\mathcal{H}^{[2]}$ to be the union of all algebraic subgroups in $\mathbb{G}_{\mathrm{m}}{}^n$ of codimension at least 2. For $\varepsilon > 0$, we let $\mathcal{H}_\varepsilon^{[2]}$ be defined similarly as in Section 1.2, that is,

$$\mathcal{H}_\varepsilon^{[2]} = \{\mathbf{u} \cdot \mathbf{v} : \mathbf{u} \in \mathcal{H}^{[2]}, \mathbf{v} \in \mathbb{G}_{\mathrm{m}}{}^n \text{ with } \mathrm{h}(\mathbf{v}) \leq \varepsilon\}.$$

We have the following result, which is a special case of [25, thàreme 1·10].

LEMMA 2·3. *Let* $g_1, \ldots, g_r \in K^*$ *and* $f_1, \ldots, f_n \in K(X)$ *be such that* $f_1, \ldots, f_n, g_1, \ldots, g_r$ *are multiplicatively independent. Let*

$$\mathcal{C} = \{(f_1(\alpha), \ldots, f_n(\alpha), g_1, \ldots, g_r) : \alpha \in \overline{K}\} \subset \mathbb{G}_m{}^{n+r}.$$

Then there exists a real number $\varepsilon > 0$ *such that* $\mathcal{C} \cap \mathcal{H}_\varepsilon^{[2]}$ *is finite.*

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

2.2. On some functional properties of rational functions

We need the following special case of the result of Young [42, corollary 1·2], which generalises the previous result of Gao [18, theorem 1·4] to multiplicative independence of consecutive iterations of rational functions over fields of characteristic zero.

LEMMA 2·4. *Let F be an arbitrary field of characteristic zero, and let $f \in F(X)$ be a rational function of degree $d \geq 2$ which is not of the form $aX^{\pm d}$. Then, for any integer $n \geq 1$, the iterates $f^{(1)}(X), \ldots, f^{(n)}(X)$ are multiplicatively independent modulo constants.*

We also need the following simple lemma.

LEMMA 2·5. *Let $f \in K(X)$ be a rational function such that it has no linear factor. Then, for any non-constant rational function $g \in K(X)$, the rational function $f \circ g$ has no linear factor.*

Proof. First, we note that it suffices to prove that for any monic irreducible factor, say $p(X)$, of either the numerator or the denominator of f, the rational function $p \circ g$ has no linear factor.

By contradiction, suppose that the rational function $p \circ g$ has a linear factor. Then, there is an element, say α, in K such that $p \circ g(\alpha) = 0$.

If $g(\alpha)$ is well-defined, then $g(\alpha) \in K$, which means that the polynomial p has a root (that is, $g(\alpha)$) in K. However, by assumption p is an irreducible polynomial over K of degree at least 2. So, we get a contradiction.

Now, if $g(\alpha)$ is not well-defined, then α is a pole of g. Write $p = X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d$ and $g = u/w$ with $u, w \in K[X]$ and $\gcd(u, w) = 1$. Since α is a pole of g, we have $w(\alpha) = 0$. Note that $p \circ g = p(u/w) = 1/w^d(u^d + a_1u^{d-1}w + \cdots + a_{d-1}uw^{d-1} + a_dw^d)$. Then, since $p \circ g(\alpha) = 0$ and $w(\alpha) = 0$, we obtain $u(\alpha) = 0$. So, α is a common root of u and w, which contradicts with $\gcd(u, w) = 1$.

Therefore, the rational function $f \circ g$ has no linear factor.

2.3. Generalised Schinzel–Tijdeman theorem

Another important tool for our results is the following general version, established in [**6**], of the Schinzel–Tijdeman theorem [**38**], which extends [7, theorem 2·3] and [9, lemma 2·8]. We present it in a simplified form, which is sufficient for our purposes.

Let K be a number field and S a finite subset of M_K containing all the infinite places. The following theorem is proved in [6, theorem 2·2].

LEMMA 2·6. *Let $f(X) = a_0X^n + \cdots + a_n \in O_S[X]$ be a polynomial of degree n and with at least two distinct roots. There is an effectively computable constant $C(f,K,S)$, depending only on f, K and S, so that the following holds: if $b \in O_S^*$ and if the equation*

$$f(x) = by^m \quad \text{in } x, y \in O_S,\ m \in \mathbb{Z}, m \geq 3, \tag{2·1}$$

has a solution (x, y) with $y \neq 0$ and $y \notin O_S^*$, then

$$m \leq C(f, K, S).$$

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

We remark that, when f has only simple roots, the result in Lemma 2·6 has been established in [9, lemma 2·8], In addition, when S only consists of infinite places, the result in Lemma 2·6 has been given in [40, theorem 10·3] (choosing $\tau = 0, z = 1, \gamma = 1, \varepsilon = b$ there).

3. *Proofs of the main results*

3.1 Preliminary discussion

Let S_Γ be the following set of places of K:

$$S_\Gamma := M_K^\infty \cup \left\{ v \in M_K^0 : v(\gamma) \neq 0 \text{ for some } \gamma \in \Gamma \right\},$$

where, as usual, $v(\gamma)$ means the additive valuation of v at γ. Note that the set S_Γ is finite, since Γ is finitely generated.

As usual, we say that a polynomial

$$f(X) = a_0 X^d + \cdots + a_{d-1} X + a_d \in K[X]$$

has bad reduction at $v \in M_K^0$ if either $v(a_i) < 0$ for some $i \geq 1$ or $v(a_0) \neq 0$; otherwise we say it has good reduction at v.

Let

$$\mathbf{f} = (f_1, \ldots, f_n) \in K[X]^n$$

be a vector of non-constant polynomials

$$f_i(X) = a_{i,0} X^{d_i} + \cdots + a_{i,d_i-1} X + a_{i,d_i} \in K[X], \quad i = 1, \ldots, n,$$

and we define

$$S_{\mathbf{f},\Gamma} = S_\Gamma \cup \{ v \in M_K^0 : \text{at least one of } f_1, \ldots, f_n \text{ has bad reduction at } v \}.$$

Note that $S_{\mathbf{f},\Gamma}$ is a finite set. Moreover, each $f_i \in O_{S_{\mathbf{f},\Gamma}}[X]$, and in fact for any $v \notin S_{\mathbf{f},\Gamma}$ we have

$$v(a_{i,0}) = 0 \qquad \text{and} \qquad v(a_{i,j}) \geq 0, \quad i = 1, \ldots, n,\ j = 1, \ldots, d_i. \tag{3·1}$$

If

$$\mathbf{f} = (f_1, \ldots, f_n) \in K(X)^n$$

is a vector of non-constant rational functions, we will use the same notation $S_{\mathbf{f},\Gamma}$ for the set including S_Γ and all the places $v \in M_K^0$ such that at least one of the numerators or denominators of $f_1, \ldots, f_n$ has bad reduction at v.

By definition, we have

$$O_{S_\Gamma} \subseteq O_{S_{\mathbf{f},\Gamma}} \qquad \text{and} \qquad \Gamma \subseteq O_{S_\Gamma}^* \subseteq O_{S_{\mathbf{f},\Gamma}}^*.$$

Note that $O_{S_{\mathbf{f},\Gamma}}^*$ is also a finitely generated subgroup of K^*. Hence, it suffices to prove the main results by replacing Γ with $O_{S_{\mathbf{f},\Gamma}}^*$. Then, in the sequel we will prove the main results by replacing $\Gamma_\varepsilon^{\mathrm{div}}$ with $O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*$, where $S_{\mathbf{f},\Gamma,\varepsilon}$ is some finite set of places containing $S_{\mathbf{f},\Gamma}$ and depending also on ε.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

3.2. Proof of Theorem 1·1

Let $\alpha \in K$ be such that there exist integers $k_1, \dots, k_n$, not all zero such that

$$f_1(\alpha)^{k_1} \cdots f_n(\alpha)^{k_n} \in \Gamma_\varepsilon^{\mathrm{div}}.$$

By Lemma 2·1 there exists $\beta \in O_{S_{\mathbf{f},\Gamma}}^*$ and $\eta \in K^*$ with $\mathrm{h}(\eta) \ll_{\varepsilon,\Gamma} 1$ such that

$$f_1(\alpha)^{k_1} \cdots f_n(\alpha)^{k_n} = \beta\eta.$$

Since $\eta \in K^*$ is of bounded height depending only on ε and Γ, by Northcott's theorem there are only finitely many such η. Thus we can enlarge the set $S_{\mathbf{f},\Gamma}$ to include all prime ideals that divide the finitely many elements η. We also include in this larger set the prime ideals outside $S_{\mathbf{f},\Gamma}$ that divide the product $\prod_{1\le i\ne j\le n} \mathrm{Res}(f_i, f_j)$ of all the resultants of f_i and f_j for $i \ne j$ (we recall that all $\mathrm{Res}(f_i, f_j)$ are $S_{\mathbf{f},\Gamma}$-integers), which are only finitely many. We denote the new set by $S_{\mathbf{f},\Gamma,\varepsilon}$ and we note that $S_{\mathbf{f},\Gamma,\varepsilon}$ is still a finite set.

By the construction of the set $S_{\mathbf{f},\Gamma,\varepsilon}$, we have

$$K^* \cap \Gamma_\varepsilon^{\mathrm{div}} \subseteq O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*.$$

Thus, it suffices to prove the desired result by replacing $\Gamma_\varepsilon^{\mathrm{div}}$ with $O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*$.

Now, we write

$$f_1(\alpha)^{k_1} \cdots f_n(\alpha)^{k_n} = \gamma, \qquad \gamma = \beta\eta \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*. \tag{3·2}$$

If $n = 1$, since f_1 is a polynomial having at least two distinct roots and $O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*$ is a finitely generated subgroup, we see that applying Lemma 2·2 to f_1 and $O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*$ gives the desired finiteness result. We thus suppose that $n \ge 2$, and that the result is valid for $n-1$, in order to apply an induction.

We note that if some $k_i = 0$, then the desired finiteness of $\alpha \in K$ satisfying (3·2) follows directly from the induction hypothesis. Hence, we can assume from now on that $k_1 \cdots k_n \ne 0$.

We now complete the proof case by case.

Case I: $\alpha \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$. □

In this case, since $\alpha \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$ and $f_i \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}[X]$ for any $i = 1, \dots, n$, we have

$$f_1(\alpha), \dots, f_n(\alpha) \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}.$$

We note that if $f_i(\alpha) \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*$ for some $i \in \{1, \dots, n\}$, then Lemma 2·2 implies the finiteness of such $\alpha \in K$ satisfying (3·2).

Thus, we now assume that $f_1(\alpha), \dots, f_n(\alpha) \notin O_{S_{\mathbf{f},\Gamma,\varepsilon}}^*$. This implies that there exists a prime ideal $\mathfrak{p} \notin S_{\mathbf{f},\Gamma,\varepsilon}$ in K such that $v_\mathfrak{p}(f_1(\alpha)) > 0$. Moreover, since $f_i(\alpha) \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$, we have $v_\mathfrak{p}(f_i(\alpha)) \ge 0$ for each $i = 2, \dots, n$.

If $k_1 k_i > 0$ for each $i = 2, \dots, n$, without loss of generality we can assume that $k_1, k_2, \dots, k_n > 0$. Then, equation (3·2) implies

$$k_1 v_\mathfrak{p}(f_1(\alpha)) + \cdots + k_n v_\mathfrak{p}(f_n(\alpha)) = 0.$$

Since $v_\mathfrak{p}(f_1(\alpha)) > 0$ and $v_\mathfrak{p}(f_i(\alpha)) \ge 0$ for each $i = 2, \dots, n$, we obtain a contradiction.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

We now assume $k_1k_i < 0$ for some $i \in \{2, \dots, n\}$. In this case, without loss of generality, we assume $k_1 > 0, \dots, k_m > 0$ and $k_{m+1} < 0, \dots, k_n < 0$ for some positive integer m. So, equation (3·2) becomes

$$f_1(\alpha)^{k_1} \cdots f_m(\alpha)^{k_m} = \gamma f_{m+1}(\alpha)^{-k_{m+1}} \cdots f_n(\alpha)^{-k_n}.$$

Then, since $v_{\mathfrak{p}}(f_1(\alpha)) > 0$ and $v_{\mathfrak{p}}(f_i(\alpha)) \geq 0$ for each $i = 2, \dots, n$, there must exist some $j \in \{m+1, \dots, n\}$ such that $v_{\mathfrak{p}}(f_j(\alpha)) > 0$. In other words, we have

$$f_1(\alpha) \equiv f_j(\alpha) \equiv 0 \pmod{\mathfrak{p}}.$$

This allows us to conclude that $v_{\mathfrak{p}}(\mathrm{Res}(f_1, f_j)) > 0$ (notice that, since $f_1, f_j \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}[X]$ and f_1 and f_j do not have common roots, we have $\mathrm{Res}(f_1, f_j) \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$ and $\mathrm{Res}(f_1, f_j) \neq 0$). By our construction of the set $S_{\mathbf{f},\Gamma,\varepsilon}$, this implies that $\mathfrak{p} \in S_{\mathbf{f},\Gamma,\varepsilon}$, which is a contradiction with the choice of $\mathfrak{p}$ above. This completes the proof of Case I.

Case II: $\alpha \notin O_{S_{\mathbf{f},\Gamma,\varepsilon}}$. □

In this case, there exists a prime ideal $\mathfrak{p}$ of the ring of integers of K such that

$$\mathfrak{p} \notin S_{\mathbf{f},\Gamma,\varepsilon} \quad \text{and} \quad v_{\mathfrak{p}}(\alpha) < 0.$$

Let $d_i = \deg f_i$, $i = 1, \dots, n$. Then, using the ultrametric inequality of non-Archimedean valuations and noticing (3.1), we directly have

$$v_{\mathfrak{p}}(f_i(\alpha)) = d_i v_{\mathfrak{p}}(\alpha) \quad \text{for } i = 1, \dots, n. \tag{3·3}$$

Considering valuations in (3·2) and using (3·3) we obtain (since $v_{\mathfrak{p}}(\gamma) = 0$ due to $\gamma \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$)

$$k_1d_1 + k_2d_2 + \cdots + k_nd_n = 0. \tag{3·4}$$

We view the above identity as a linear Diophantine equation with unknowns $k_1, \dots, k_n$ in $\mathbb{Z}$. Then, we have a basis of the integer solutions $(k_1, k_2, \dots, k_n)$ of the equation (3·4), say,

$$(t_{i,1}, t_{i,2}, \dots, t_{i,n}), \quad i = 1, \dots, n-1.$$

Therefore, $k_1, k_2, \dots, k_n$ can be expressed as

$$k_j = \sum_{i=1}^{n-1} s_i t_{i,j}, \quad j = 1, \dots, n,$$

for some integers $s_1, \dots, s_{n-1}$. Substituting this into the equation (3·2), we obtain

$$\left(\prod_{j=1}^{n} f_j(\alpha)^{t_{1,j}}\right)^{s_1} \cdots \left(\prod_{j=1}^{n} f_j(\alpha)^{t_{n-1,j}}\right)^{s_{n-1}} = \gamma. \tag{3·5}$$

Now, we let

$$F(X) = \prod_{j=1}^{n} f_j(X)^{t_{1,j}},$$

where the exponent vector $(t_{1,1}, \dots, t_{1,n})$ is non-zero by its choice above.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

For any prime $\mathfrak{q} \notin S_{\mathbf{f},\Gamma,\varepsilon}$, if $v_{\mathfrak{q}}(\alpha) < 0$, then (3·3) holds and we have

$$\begin{aligned} v_{\mathfrak{q}}(F(\alpha)) &= \sum_{j=1}^{n} t_{1,j} v_{\mathfrak{q}}(f_j(\alpha)) \\ &= (t_{1,1}d_1 + t_{1,2}d_2 + \cdots + t_{1,n}d_n) v_{\mathfrak{q}}(\alpha) = 0, \end{aligned} \tag{3·6}$$

since $(t_{1,1}, t_{1,2}, \ldots, t_{1,n})$ is a solution to (3·4).

For any prime $\mathfrak{q} \notin S_{\mathbf{f},\Gamma,\varepsilon}$, if $v_{\mathfrak{q}}(\alpha) \geq 0$, then by (3·1) we have $v_{\mathfrak{q}}(f_i(\alpha)) \geq 0$ for each $i = 1, \ldots, n$.

If there exists some prime $\mathfrak{q} \notin S_{\mathbf{f},\Gamma,\varepsilon}$ such that $v_{\mathfrak{q}}(\alpha) \geq 0$ and moreover $v_{\mathfrak{q}}(f_i(\alpha)) > 0$, $v_{\mathfrak{q}}(f_j(\alpha)) > 0$ for some $i \neq j$, then by the same discussion as in the last part of Case I we arrive to a contradiction.

If there exists some prime $\mathfrak{q} \notin S_{\mathbf{f},\Gamma,\varepsilon}$ such that $v_{\mathfrak{q}}(\alpha) \geq 0$ and moreover $v_{\mathfrak{q}}(f_i(\alpha)) > 0$ for exactly one i for $i = 1, \ldots, n$, say $v_{\mathfrak{q}}(f_1(\alpha)) > 0$ and $v_{\mathfrak{q}}(f_i(\alpha)) = 0$ for each $i = 2, \ldots, n$, then by (3·5) we obtain

$$s_1 t_{1,1} + \cdots + s_{n-1} t_{n-1,1} = 0,$$

which however contradicts with $k_1 \neq 0$ because $k_1 = s_1 t_{1,1} + \cdots + s_{n-1} t_{n-1,1}$.

Hence, we may assume that for any prime $\mathfrak{q} \notin S_{\mathbf{f},\Gamma,\varepsilon}$, if $v_{\mathfrak{q}}(\alpha) \geq 0$, then $v_{\mathfrak{q}}(f_i(\alpha)) = 0$ for each $i = 1, \ldots, n$. In this case, we have $v_{\mathfrak{q}}(F(\alpha)) = 0$. Combining this with (3·6), we have $v_{\mathfrak{q}}(F(\alpha)) = 0$ for any prime $\mathfrak{q} \notin S_{\mathbf{f},\Gamma,\varepsilon}$, and thus $F(\alpha) \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$. Now, the desired result follows directly from Lemma 2·2 (which we can apply, since f_i, $i = 1, \ldots, n$, has at least two distinct roots and they are pairwise coprime, and therefore, F has at least two distinct roots or two distinct poles). This completes the proof.

3.3. Proof of Theorem 1·2

First, we assume that the rational functions $f_1, f_2, \ldots, f_n$ all have no linear factor.

Let $g_1, \ldots, g_m$ be all the distinct monic irreducible factors (over K) in the numerators and denominators of the rational functions $f_1, f_2, \ldots, f_n$. So, by assumption, the irreducible polynomials $g_1, \ldots, g_m$ are all of degree at least two. Then, for each f_i, $1 \leq i \leq n$, we can write

$$f_i = a_i \prod_{j=1}^{m} g_j^{e_{ij}}, \quad a_i \in K^*, \tag{3·7}$$

for some integers $e_{i1}, \ldots, e_{im}$.

Let $\alpha \in K$ be such that there exist integers $k_1, \ldots, k_n$, not all zero such that

$$f_1(\alpha)^{k_1} \cdots f_n(\alpha)^{k_n} \in \Gamma_{\varepsilon}^{\mathrm{div}}.$$

As in (3·2), we can write

$$f_1(\alpha)^{k_1} \cdots f_n(\alpha)^{k_n} = \gamma, \qquad \gamma \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}, \tag{3·8}$$

where the set $S_{\mathbf{f},\Gamma,\varepsilon}$ is defined as in the proof of Theorem 1·1, however without including the prime ideals outside $S_{\mathbf{f},\Gamma}$ that divide the product $\prod_{1 \leq i \neq j \leq n} \mathrm{Res}(f_i, f_j)$ of all the resultants of f_i and f_j for $i \neq j$, because f_i and f_j might not be polynomials.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

By the discussion in Section 3.1, we know that $a_i \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$ for each $i = 1, \dots, n$. Hence, combining (3·8) with (3·7), we get that for some $\gamma' \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$,

$$g_1(\alpha)^{k_1 e_{11} + \cdots + k_n e_{n1}} \cdots g_m(\alpha)^{k_1 e_{1m} + \cdots + k_n e_{nm}} = \gamma'. \tag{3·9}$$

If for each $1 \le j \le m$, $k_1 e_{1j} + \cdots + k_n e_{nj} = 0$, then this means that $f_1^{k_1} \cdots f_n^{k_n}$ is a constant, which contradicts with the assumption that $f_1, \dots, f_n$ are multiplicatively independent modulo constants.

So, we must have that $k_1 e_{1j} + \cdots + k_n e_{nj} \neq 0$ for some $1 \le j \le m$. Then, in view of (3·9) and noticing that $g_1, \dots, g_m$ are pairwise distinct irreducible polynomials of degree at least 2, we obtain directly the desired finiteness result by applying Theorem 1·1 to the polynomials $g_1, \dots, g_m$. This completes the proof of the case when $f_1, f_2, \dots, f_n$ all have no linear factor.

Now, without loss of generality, we assume that for each $f_i, i = 1, 2, \dots, n$, both its numerator and denominator have linear factors.

Then, for each $f_i, i = 1, 2, \dots, n$, we write

$$f_i = a_i f_{i1} f_{i2}, \quad a_i \in K^*,$$

where $f_{i1} \in K(X)$ is monic and only has linear factors, and $f_{i2} \in K(X)$ is monic and only has irredicible factors of degree at least two; and moreover, we write

$$f_{i1} = \frac{h_{i1}}{h_{i2}}, \quad h_{i1}, h_{i2} \in K[X], \ \gcd(h_{i1}, h_{i2}) = 1.$$

By assumption, for each $i = 1, 2, \dots, n$, both h_{i1} and h_{i2} have at least two distinct linear factors and they only have linear factors. Moreover, since we have assumed that $f_1, f_2, \dots, f_n$ have distinct linear factors, we know that $h_{11}, h_{12}, \dots, h_{n1}, h_{n2}$ are pairwise coprime.

Let $g_1, \dots, g_m$ (assume $m \ge 1$) be all the distinct monic irreducible factors (over K) in the numerators and denominators of the rational functions $f_{12}, \dots, f_{n2}$.

By assumption, the irreducible polynomials $g_1, \dots, g_m$ are all of degree at least two. So, the polynomials $h_{11}, h_{12}, \dots, h_{n1}, h_{n2}, g_1, \dots, g_m$ are pairwise coprime.

Then, for each $f_i, 1 \le i \le n$, we can write

$$f_i = a_i h_{i1} h_{i2}^{-1} \prod_{j=1}^{m} g_j^{e_{ij}}, \quad a_i \in K^*, \tag{3·10}$$

for some integers $e_{i1}, \dots, e_{im}$.

As in (3·9), combining (3·8) with (3·10) we can get that for some $\gamma' \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$,

$$\prod_{i=1}^{n} h_{i1}(\alpha)^{k_i} h_{i2}(\alpha)^{-k_i} \cdot \prod_{j=1}^{m} g_j(\alpha)^{k_1 e_{1j} + \cdots + k_n e_{nj}} = \gamma'. \tag{3·11}$$

Then, in view of (3·11) and noticing that the integers $k_1, \dots, k_n$ are not all zero, we obtain directly the desired finiteness result by applying Theorem 1·1 to the polynomials $h_{11}, h_{12}, \dots, h_{n1}, h_{n2}, g_1, \dots, g_m$. This completes the proof.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

3.4. Proof of Corollary 1·4

First, we assume that $f \in K[X]$ and 0 is not a periodic point of f. Since 0 is not a periodic point of f, we have that for any integer $n \geq 1, f^{(n)}(0) \neq 0$, which means that $f^{(n)}$ has non-zero constant term. So, all the iterates of f are pairwise coprime. In addition, since f has at least two distinct roots, it is easy to see that each iterate of f also has at least two distinct roots. Hence, by Theorem 1·1 we know that there are only finitely many elements $\beta \in K$ such that $f^{(1)}(\beta), \ldots, f^{(n)}(\beta)$ are multiplicatively dependent modulo $\Gamma_{\varepsilon}^{\mathrm{div}}$.

Now, we assume that f has no linear factor. Then, by Lemma 2·5, the iterates $f^{(1)}, \ldots, f^{(n)}$ all have no linear factor. Moreover, it follows directly from Lemma 2·4 that the iterates $f^{(1)}, \ldots, f^{(n)}$ are multiplicatively independent modulo constants. So, using Theorem 1·2 we get that there are only finitely many elements $\beta \in K$ such that $f^{(1)}(\beta), \ldots, f^{(n)}(\beta)$ are multiplicatively dependent modulo $\Gamma_{\varepsilon}^{\mathrm{div}}$.

So, for proving the desired result, it suffices to fix such an element β and show that there are only finitely many $\alpha \in K$ such that $f^{(m)}(\alpha) = \beta$ for some integer $m \geq 0$. Indeed, this follows directly from [9, lemma 2·3] and the well-known fact that f has only finitely many preperiodic points lying in K.

3.5 Proof of Theorem 1·5

The proof follows similar ideas as in the proof of [9, theorem 1·7].

Let $\alpha \in K$ be such that there exist integers k_1, k_2, not both zero, such that

$$f_1(\alpha)^{k_1} f_2(\alpha)^{k_2} \in \Gamma_{\varepsilon}^{\mathrm{div}}.$$

As in the proof of Theorem 1·1, we enlarge the set $S_{\mathbf{f},\Gamma}$ (in this case $\mathbf{f} = (f_1, f_2)$) to a larger set $S_{\mathbf{f},\Gamma,\varepsilon}$ such that

$$f_1(\alpha)^{k_1} f_2(\alpha)^{k_2} = \gamma \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}. \tag{3·12}$$

Also, as in the proof of Theorem 1·1 we can assume that $k_1 k_2 \neq 0$. From (3·12) and the power saturation of $O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$ in K^*, we see that

$$\gamma = \beta^{\gcd(k_1,k_2)} \quad \text{for some } \beta \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}.$$

This allows us to take the $\gcd(k_1, k_2)$-root of (3·12), so without loss of generality we can assume that

$$\gcd(k_1, k_2) = 1.$$

We now complete the proof case by case.

Case I: $\alpha \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$. □

In this case, we have $f_1(\alpha), f_2(\alpha) \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$. We note that if $f_1(\alpha) \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$ or $f_2(\alpha) \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$, then Lemma 2·2 implies the finiteness of such $\alpha \in K$ satisfying (3·12).

Thus, we can assume that $f_1(\alpha), f_2(\alpha) \notin O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$. This implies that there exists a prime ideal $\mathfrak{p}$ of K such that the additive valuation $v_{\mathfrak{p}}(f_1(\alpha)) > 0$. Moreover, since $f_2(\alpha) \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$, we have $v_{\mathfrak{p}}(f_2(\alpha)) \geq 0$.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

If $k_1k_2 > 0$, then we can assume that $k_1, k_2 > 0$. In this case, since equation (3·12) implies

$$k_1 v_{\mathfrak{p}}(f_1(\alpha)) + k_2 v_{\mathfrak{p}}(f_2(\alpha)) = 0,$$

we obtain a contradiction by noticing $v_{\mathfrak{p}}(f_1(\alpha)) > 0$ and $v_{\mathfrak{p}}(f_2(\alpha)) \geq 0$.

We now assume $k_1k_2 < 0$. Moreover, we can assume $k_1 > 0$ and $k_2 < 0$ (similar discussion applies for $k_1 < 0$ and $k_2 > 0$). Since $\gcd(k_1, k_2) = 1$, there exist integers s, t such that

$$sk_1 + tk_2 = 1.$$

Then, using (3·12), we have

$$\begin{aligned} f_1(\alpha) &= f_1(\alpha)^{sk_1+tk_2} = \gamma^s (f_1(\alpha)^{-t} f_2(\alpha)^s)^{-k_2}, \\ f_2(\alpha) &= f_2(\alpha)^{sk_1+tk_2} = \gamma^t (f_1(\alpha)^{-t} f_2(\alpha)^s)^{k_1}. \end{aligned} \tag{3·13}$$

We note that, since $f_1(\alpha) \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$, $\gamma \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$ and $-k_2 > 0$, we have $f_1(\alpha)^{-t} f_2(\alpha)^s \in O_{S_{\mathbf{f},\Gamma,\varepsilon}}$.

If $f_1(\alpha)^{-t} f_2(\alpha)^s \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$, then by (3·13) we obtain that $f_1(\alpha) \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$, which contradicts our assumption above. Thus, $f_1(\alpha)^{-t} f_2(\alpha)^s \notin O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$. Then, by Lemma 2·6 (with $y = f_1(\alpha)^{-t} f_2(\alpha)^s$ and noticing $\gamma \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$), the exponent $-k_2$ is bounded above only in terms of f_1, f_2, K, Γ and ε. Similarly, we obtain that the exponent k_1 is also bounded above only in terms of f_1, f_2, K, Γ and ε. Hence, in (3·12) there are only finitely many choices of the two exponents k_1, k_2. Then, fixing k_1, k_2 and applying Lemma 2·2 to the rational function $f_1^{k_1} f_2^{k_2}$, we obtain the desired finiteness result, where we need to use the assumption on f_1 and f_2 that they can not multiplicatively generate a power of a linear fractional function. This completes the proof of Case I.

Case II: $\alpha \notin O_{S_{\mathbf{f},\Gamma,\varepsilon}}$. □

In this case, as in the proof of Theorem 1·1, we can choose a prime ideal $\mathfrak{p}$ of the ring of integers of K such that

$$\mathfrak{p} \notin S_{\mathbf{f},\Gamma,\varepsilon} \quad \text{and} \quad v_{\mathfrak{p}}(\alpha) < 0.$$

Let $d_i = \deg f_i$, $i = 1, 2$. Then, using the ultrametric inequality of non-Archimedean valuations and noticing (3·1), we directly have

$$v_{\mathfrak{p}}(f_i(\alpha)) = d_i v_{\mathfrak{p}}(\alpha) \quad \text{for } i = 1, 2. \tag{3·14}$$

Considering valuations in (3·12) and using (3.14) we obtain (since $v_{\mathfrak{p}}(\gamma) = 0$ due to $\gamma \in O^*_{S_{\mathbf{f},\Gamma,\varepsilon}}$)

$$k_1 d_1 + k_2 d_2 = 0.$$

Since $\gcd(k_1, k_2) = 1$, this implies that $k_1 \mid d_2$ and $k_2 \mid d_1$. Thus we can assume that both k_1 and k_2 are fixed. Then, as in Case I, the desired finiteness result follows from Lemma 2·2. This completes the proof.

3.6. Proof of Theorem 1·6

The proof follows directly from Maurin's result (that is, Lemma 2·3). Indeed, let r be the rank of Γ modulo torsion and let $g_1, \ldots, g_r \in \Gamma$ be its generators, and thus, they are

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

multiplicatively independent elements. We define the parametric curve

$$\mathcal{C} = \{(\alpha, f_1(\alpha), \dots, f_n(\alpha), g_1, \dots, g_r) : \alpha \in \overline{K}\} \subset \mathbb{G}_{\mathrm{m}}{}^{n+r+1}.$$

We choose ε to be half of the size of the real ε from Lemma 2·3.

For an element $\alpha \in \Gamma_\varepsilon^{\mathrm{div}}$, assume that $f_1(\alpha), \dots, f_n(\alpha)$ are multiplicatively dependent modulo $\Gamma_\varepsilon^{\mathrm{div}}$. Since $\alpha \in \Gamma_\varepsilon^{\mathrm{div}}$, there exist a non-zero vector $(k_0, \dots, k_r) \in \mathbb{Z}^{r+1}$, $k_0 \neq 0$, such that

$$\alpha^{k_0} g_1^{k_1} \cdots g_r^{k_r} = \beta^{k_0}$$

for some $\beta \in \overline{K}^*$ with $\mathrm{h}(\beta) \leq \varepsilon$, implying that

$$\frac{\alpha^{k_0}}{\beta^{k_0}} g_1^{k_1} \cdots g_r^{k_r} = 1. \tag{3·15}$$

Moreover, since $f_1(\alpha), \dots, f_n(\alpha)$ are multiplicatively dependent modulo $\Gamma_\varepsilon^{\mathrm{div}}$, there exist some positive integer t and a non-zero vector $(\ell_1, \dots, \ell_{n+r}) \in \mathbb{Z}^{n+r}$ such that

$$f_1(\alpha)^{t\ell_1} \cdots f_n(\alpha)^{t\ell_n} g_1^{\ell_{n+1}} \cdots g_r^{\ell_{n+r}} = \gamma^t$$

for some $\gamma \in \overline{K}^*$ with $\mathrm{h}(\gamma) \leq \varepsilon$, implying that (without loss of generality, we assume $\ell_1 \cdots \ell_n \neq 0$)

$$\frac{f_1(\alpha)^{t\ell_1}}{\gamma^{t\ell_1/n\ell_1}} \cdots \frac{f_n(\alpha)^{t\ell_n}}{\gamma^{t\ell_n/n\ell_n}} g_1^{\ell_{n+1}} \cdots g_r^{\ell_{n+r}} = 1. \tag{3·16}$$

Therefore, the point

$$\left(\frac{\alpha}{\beta}, \frac{f_1(\alpha)}{\gamma^{1/n\ell_1}}, \dots, \frac{f_n(\alpha)}{\gamma^{1/n\ell_n}}, g_1, \dots, g_r\right)$$

satisfies the multiplicative dependence relations (3.15) and (3.16), which have linearly independent vectors of exponents. Moreover,

$$\begin{aligned}&(\alpha, f_1(\alpha), \dots, f_n(\alpha), g_1, \dots, g_r)\\ &= \left(\frac{\alpha}{\beta}, \frac{f_1(\alpha)}{\gamma^{1/n\ell_1}}, \dots, \frac{f_n(\alpha)}{\gamma^{1/n\ell_n}}, g_1, \dots, g_r\right) \cdot (\beta, \gamma^{1/n\ell_1}, \dots, \gamma^{1/n\ell_n}, 1, \dots, 1)\end{aligned}$$

is a point on $\mathcal{C}$ with

$$\begin{aligned}\mathrm{h}(\beta, \gamma^{1/n\ell_1}, \dots, \gamma^{1/n\ell_n}, 1, \dots, 1) &:= \mathrm{h}(\beta) + \mathrm{h}(\gamma^{1/n\ell_1}) + \cdots + \mathrm{h}(\gamma^{1/n\ell_n})\\ &\leq \mathrm{h}(\beta) + \mathrm{h}(\gamma) \leq 2\varepsilon.\end{aligned}$$

We also note that by assumption, the functions $X, f_1, \dots, f_n, g_1, \dots, g_r$ are multiplicatively independent. Hence, the desired result follows directly from Lemma 2·3.

Acknowledgements. The authors are grateful to the referee for a careful reading of the manuscript and valuable comments. The research of Attila Bérczes was supported in part by grants K128088 and ANN130909 of the Hungarian National Foundation for Scientific Research and by the project EFOP-3.6.1-16-2016-00022 co-financed by the European Union and the European Social Fund. Kálmán Győry was supported in part by grants K128088 and ANN130909 of the Hungarian National Foundation for Scientific Research. Jorge Mello

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

and Alina Ostafe were partially supported by the Australian Research Council Grants DP180100201 and DP200100355. Min Sha was supported by the Guangdong Basic and Applied Basic Research Foundation (No. 2022A1515012032) and also by the Australian Research Council Grant DE190100888. Alina Ostafe also gratefully acknowledges the generosity and hospitality of the Max Planck Institute for Mathematics where parts of her work on this project were developed.

REFERENCES

[1] I. ALIEV and C. J. SMYTH. Solving algebraic equations in roots of unity. *Forum Math.* **24** (2012), 641–665.
[2] F. AMOROSO. On a conjecture of G. Rémond. Ann. Scuola Norm. Sup. Pise Cl. *Sci.* **15** (2016), 599–608.
[3] F. AMOROSO and E. VIADA. Small points on subvarieties of a torus. *Duke Math. J.* **150** (2009), 407–442.
[4] F. BARROERO, L. CAPUANO, L. MÉRAI, A. OSTAFE and M. SHA. Multiplicative and linear dependence in finite fields and on elliptic curves modulo primes. *Int. Math. Res. Not.* 2022 (2022), 16094–16137.
[5] F. BARROERO and M. SHA. Torsion points with multiplicatively dependent coordinates on elliptic curves. *Bull. London Math. Soc.* **52** (2020), 807–815.
[6] A. BÉRCZES, Y. BUGEAUD, K. GYŐRY, J. MELLO, A. OSTAFE and M. SHA. Explicit bounds for the solutions of superelliptic equations over number fields. *Forum Math.* 2024, https://doi.org/10.1515/forum-2023-0381.
[7] A. BÉRCZES, J.-H. EVERTSE and K. GYŐRY. Effective results for hyper- and superelliptic equations over number fields. *Publ. Math. Debrecen* **82** (2013), 727–756.
[8] A. BÉRCZES, J.-H. EVERTSE, K. GYŐRY and C. PONTREAU. Effective results for points on certain subvarieties of tori. *Math. Proc. Camb. Phil. Soc.* 147 (2009), 69–94.
[9] A. BÉRCZES, A. OSTAFE, I. E. SHPARLINSKI and J. H. SILVERMAN. Multiplicative dependence among iterated values of rational functions modulo finitely generated groups. *Int. Math. Res. Not.* 2021 (2021), 9045–9082.
[10] F. BEUKERS and C. J. SMYTH. Cyclotomic points on curves. Number Theory for the Millenium (Urbana, Illinois, 2000), I (A. K. Peters, 2002), 67–85.
[11] E. BOMBIERI, P. HABEGGER, D. MASSER and U. ZANNIER. A note on Maurin's theorem. *Rend. Lincei Mat. Appl.* **21** (2010), 251–260.
[12] E. BOMBIERI, D. MASSER and U. ZANNIER. Intersecting a curve with algebraic subgroups of multiplicative groups. *Int. Math. Res. Not.* 1999 (1999), 1119–1140.
[13] E. BOMBIERI and U. ZANNIER. Algebraic points on subvarieties of $\mathbb{G}_m^n$. *Int. Math. Res. Not.* 1995 (1995), 333–347.
[14] A. DUBICKAS and M. SHA. Multiplicative dependence of the translations of algebraic numbers. *Rev. Mat. Iberoam.* **34** (2018), 1789–1808.
[15] R. DVORNICICH and U. ZANNIER. Cyclotomic diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps). *Duke Math. J.* **139** (2007), 527–554.
[16] J.-H. EVERTSE. Points on subvarieties of tori. *A panorama of number theory or the view from Baker's garden (Zürich, 1999)* (Cambridge University Press, 2002), 214–230.
[17] G. FALTINGS. Endlichkeitssätze fur abelsche Varietäten über Zahlkorpern. *Invent. Math.* **73** (1983), 349–366.
[18] S. GAO. Elements of provable high order in finite fields. *Proc. Amer. Math. Soc.* 127 (1999), 1615–1623.
[19] S. V. KONYAGIN, M. SHA, I. E. SHPARLINSKI and C. L. STEWART. On the distribution of multiplicatively dependent vectors. *Math. Res. Lett.* **30** (2023), 509–540.
[20] M. LAURENT. Equations diophantiennes exponentielles. *Invent. Math.* **78** (1984), 299–327.
[21] P. LIARDET. Sur une conjecture de Serge Lang. *Astérisque* **24-25** (1975), 187–210.
[22] J. H. LOXTON and A. J. VAN DER POORTEN. Multiplicative dependence in number fields. *Acta Arith.* **42** (1983), 291–302.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press

[23] C. MARTINEZ. The number of maximal torsion cosets on subvarieties of tori. *J. Reine Angew. Math.* **755** (2019), 10–126.
[24] G. MAURIN. Courbes algébriques et équations multiplicatives. *Math. Ann.* **341** (2008), 789–824.
[25] G. MAURIN. Équations multiplicatives sur les sous-variétés des tores. *Int. Math. Res. Not.* 2011 (2011), 5259–5366.
[26] B. MAZUR. Abelian varieties and the Mordell–Lang conjecture. Model theory, algebra, and geometry. *Math. Sci. Res. Inst. Publ.* 39 (Cambridge University Press, 2000), 199–227.
[27] A. OSTAFE, M. SHA, I. E. SHPARLINSKI and U. ZANNIER. On abelian multiplicatively dependent points on a curve in a torus. *Q. J. Math.* **69** (2018), 391–401.
[28] A. OSTAFE, M. SHA, I. E. SHPARLINSKI and U. ZANNIER. On multiplicative dependence of values of rational functions and a generalisation of the Northcott theorem. *Michigan Math. J.* **68** (2019), 385–407.
[29] A. OSTAFE and I. E. SHPARLINSKI. Orbits of algebraic dynamical systems in subgroups and subfields. Number Theory - Diophantine problems, uniform distribution and applications, C. ELSHOLTZ and P. GRABNER (Eds.) (Springer, 2017), 347–368.
[30] A. OSTAFE and I. E. SHPARLINSKI. On the Skolem problem and some related questions for parametric families of linear recurrence sequences. *Canad. J. Math.* **74** (2022), 773–792.
[31] F. PAPPALARDI, M. SHA, I. E. SHPARLINSKI and C. L. STEWART. On multiplicatively dependent vectors of algebraic numbers. *Trans. Amer. Math. Soc.* **370** (2018), 6221–6244.
[32] C. PONTREAU. A Mordell–Lang plus Bogolomov type result for curves in $\mathbb{G}_m^2$. *Monatsh. Math.* **157** (2009), 267–281.
[33] B. POONEN. Mordell–Lang plus Bogomolov. *Invent. Math.* **137** (1999), 413–425.
[34] L. POTTMEYER. Fields generated by finite rank subgroups of $\overline{\mathbb{Q}}^*$. *Int. J. Number Theory* **17** (2021), 1079–1089.
[35] A. J. VAN DER POORTEN and J. H. LOXTON. Multiplicative relations in number fields. *Bull. Austral. Math. Soc.* **16** (1977), 83–98.
[36] G. RÉMOND. Sur les sous-variétés des tores. *Compositio. Math.* **134** (2002), 337–366.
[37] G. RÉMOND. Généralisations du problème de Lehmer et applications à la conjecture de Zilber–Pink. *Panor. Synth.* **52** (2017), 243–284.
[38] A. SCHINZEL and R. TIJDEMAN. On the equation $y^m = P(x)$. *Acta Arith.* **31** (1976), 199–204.
[39] W. M. SCHMIDT. Heights of points on subvarieties of $\mathbb{G}_m^n$. Number Theory (Paris, 1993–1994). London Math. Soc. Lecture Note Ser. 235 (Cambridge University Press, 1996), 157–187.
[40] T. N. SHOREY and R. TIJDEMAN. *Exponential Diophantine Equations*. (Cambridge University Press, Cambridge, 1986).
[41] C. L. STEWART. On heights of multiplicatively dependent algebraic numbers. *Acta Arith.* **133** (2008), 97–108.
[42] M. YOUNG. On multiplicative independence of rational function iterates. *Monatsh. Math.* **192** (2020), 225–247.

https://doi.org/10.1017/S0305004124000173 Published online by Cambridge University Press