The Quarterly Journal of Mathematics Advance Access published on September 26, 2017
Quart. J. Math. 69 (2018), 391–401; doi:10.1093/qmath/hax045

ON ABELIAN MULTIPLICATIVELY DEPENDENT POINTS ON A CURVE IN A TORUS

by ALINA OSTAFE[†]

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

MIN SHA[‡]
(*Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*)

IGOR E. SHPARLINSKI[§]
(*School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia*)

and UMBERTO ZANNIER[**]
(*Scuola Normale Superiore, Piazza dei Cavalieri, 7, 56126 Pisa, Italy*)

[Received 16 May 2017. Revised 23 August 2017]

Abstract

We show, under some natural conditions, that the set of abelian (and thus also cyclotomic) multiplicatively dependent points on an irreducible curve over a number field is a finite union of preimages of roots of unity by a certain finite set of primitive characters from $\mathbb{G}_{\mathrm{m}}^n$ to $\mathbb{G}_{\mathrm{m}}$ restricted to the curve, and a finite set. We also introduce the notion of primitive multiplicative dependence and obtain a finiteness result for primitively multiplicatively dependent points defined over a so-called Bogomolov extension of a number field.

1. Introduction

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. Let n be a positive integer with $n \geq 2$. The points in $\mathbb{G}_{\mathrm{m}}^n$ whose coordinates are roots of unity are called torsion points. In 1960s, Lang [**9**] conjectured that if a complex plane irreducible curve contains infinitely many torsion points, then the curve is a torsion coset of $\mathbb{G}_{\mathrm{m}}^2$. This was soon confirmed by Ihara *et al*., see [**9**] for more details.

So far, there are two ways to generalize the above result. The first is to describe torsion points on an algebraic variety of higher dimension. This leads to the torsion points theorem proved independently by Laurent [**10**] and Sarnak and Adams [**12**]. The theorem asserts that the torsion points

[†]E-mail: alina.ostafe@unsw.edu.au

[‡]Coresponding author. E-mail: shamin2010@gmail.com

[§]E-mail: igor.shparlinski@unsw.edu.au

[**]E-mail: u.zannier@sns.it

in a subvariety $Y \subseteq \mathbb{G}_{\mathrm{m}}^n$ all lie and are Zariski dense in a finite number of torsion cosets contained in Y. Note that the torsion points constitute a multiplicative group of rank 0. So, the other way is to consider multiplicative groups of higher ranks. This was initiated by Bombieri *et al.* [5]. We refer to [16] for more historic notes.

More precisely, the paper [5] studies the intersection of a geometrically irreducible algebraic curve $X \subseteq \mathbb{G}_{\mathrm{m}}^n$, defined over a number field, and the union of proper algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^n$. As is well known (see, for example [4, Corollary 3.2.15]), each such subgroup H is defined by a finite set of equations of the shape $x_1^{a_1} \cdots x_n^{a_n} = 1$, with integer exponents not all zero. Hence, the above intersection consists of the points $P = (\xi_1, \ldots, \xi_n) \in X$ such that the coordinates $\xi_1 = x_1(P), \ldots, \xi_n = x_n(P)$ are all non-zero and are *multiplicatively dependent*. In the sequel, we call such points just *dependent*.

Let us note that any map $(x_1, \ldots, x_n) \mapsto x_1^{a_1} \cdots x_n^{a_n}$, denoted by $\mathbf{x} \to \mathbf{x}^{\mathbf{a}}$ in the sequel, is a (rational) homomorphism from $\mathbb{G}_{\mathrm{m}}^n$ to $\mathbb{G}_{\mathrm{m}}$, often called a *character*, which is non-trivial if and only if it is surjective, and in fact all rational homomorphisms $\mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}$ are of this shape; see [4, Proposition 3.2.17]. The set of dependent points in $\mathbb{G}_{\mathrm{m}}^n$ is just the union of the kernels of these non-trivial characters.

Coming back to X, one may assume for the problems in question that it is not contained in any proper algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^n$, since otherwise a (fixed) dependence occurs for all points of X. Under this assumption, $X \cap H$ is finite for any such algebraic subgroup H, so that it consists of points defined over $\overline{\mathbb{Q}}$. Also, on varying H, it is easy to see that the union of these intersections, that is, the set of dependent points on X, is infinite.

It has been proved in [5, Theorem 1], that, under the assumption that X *is not contained in any translate of a proper algebraic subgroup of* $\mathbb{G}_{\mathrm{m}}^n$, the absolute logarithmic *Weil* height in $X \cap H$ is bounded independently of H, see [4, 17] for a background on heights.

This more stringent assumption means that no equation $x_1^{a_1} \cdots x_n^{a_n} = c$, for a constant c and integers a_i not all zero, can hold identically on X, that is, X is not contained in any fibre of a non-trivial rational character to $\mathbb{G}_{\mathrm{m}}$. In [5], this hypothesis has been noted to be necessary for the bounded-height conclusion. Throughout the paper, we always assume this condition for X.

Now, one can ask what can be further said on restricting the dependent points of X to be defined over proper subfields of $\overline{\mathbb{Q}}$. For instance, over any number field, or even just imposing some bound for the degree over $\mathbb{Q}$, the mentioned bounded-height result of [5] implies that there can be only finitely many such points on X which are dependent, because of the *Northcott theorem*, see [4, Theorem 1.6.8].

Other fields relevant to this context are the *maximal cyclotomic fields* K_{c}, that is, fields obtained by adjoining all roots of unity to a number field K. This is especially for the reason that any point with a coordinate which is a root of unity is automatically dependent. The goal of this paper is, roughly, to describe the structure of abelian (and thus also cyclotomic) points on X which are dependent. Note for instance that the said result of [5] does not lead us to expect automatically finiteness, since the Northcott Property certainly fails for the maximal cyclotomic fields.

In fact, a situation which generates infinitely many dependent cyclotomic points on X is as follows. Suppose that the character $\varphi\colon \mathbf{x} = (x_1, \ldots, x_n) \to \mathbf{x}^{\mathbf{a}}$, where $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$, restricts on X to a birational correspondence $\varphi_X\colon X \to \mathbb{G}_{\mathrm{m}}$. Then, the inverse image $\varphi_X^{-1}(\zeta)$ of any root of unity ζ 'usually' consists of one point $P \in X$, hence necessarily defined over a cyclotomic extension, and certainly by definition this point is dependent, since $\varphi(P)^m = 1$ for some $m > 0$. More generally, if φ_X is a factor of an isogeny $\varphi_X \circ \rho\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$ (with ρ some birational map $\mathbb{G}_{\mathrm{m}} \to X$ defined over K_{c}), again the inverse image of any root of unity produces cyclotomic points, automatically dependent.

More precisely, here we obtain the following result: in Theorem 2.1, we prove that the above situation characterizes, in finite terms, all of the cyclotomic-dependent points in X, and in fact we obtain a more general result for *abelian* dependent points in X, that is, for points from the abelian

closure K_{ab} of K. In Theorem 2.10, we obtain a similar result for a more stringent relation, however, for an even broader class of fields, called fields with the Bogomolov property.

For possible applications of our results, see Remark 4.2 below and [**11**].

2. Main results

To state in precision our results, let K be a number field and let $X \subseteq \mathbb{G}_{\mathrm{m}}^n$ be a geometrically irreducible curve defined over K. Let us denote by $U \subset \overline{\mathbb{Q}}$ the set of all roots of unity. As before, we use K_{c} to denote the maximal cyclotomic extension of K, that is, $K_{\mathrm{c}} = K(U)$ and use K_{ab} to denote the maximal abelian extension over K which includes, but is generally much larger than, K_{c} (if $K \neq \mathbb{Q}$).

We also denote by $\varphi_X \colon X \to \mathbb{G}_{\mathrm{m}}$ the restriction to X of the character φ on $\mathbb{G}_{\mathrm{m}}^n$. Recall that a character is called *primitive* if it is not of the shape ψ^m for a character ψ and an integer $m > 1$.

As usual, for any field L with $K \subseteq L$, we write $X(L)$ for the set of L-rational points on X.

Throughout the paper, the 'height' means the 'absolute logarithmic Weil height', which we denote by h: $\overline{\mathbb{Q}} \to \mathbb{R} \cap [0, \infty)$; see [**4**, **17**].

Let Φ_X be the set of primitive characters $\varphi \colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}$ with the property that there exists a birational isomorphism $\rho \colon \mathbb{G}_{\mathrm{m}} \to X$ such that $\varphi_X \circ \rho$ is an isogeny of $\mathbb{G}_{\mathrm{m}}$.

We also use $\Phi_{X,\mathrm{c}}$ to denote the subset of Φ_X consisting of those characters for which ρ can be defined over K_{c}

We now present our main result:

THEOREM 2.1 *Suppose that X is not contained in any translate of a proper algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^n$. Then, Φ_X is a finite set, and the set of dependent points in $X(K_{\mathrm{ab}})$ is the union of the set $\bigcup_{\varphi \in \Phi_{X,\mathrm{c}}} \varphi_X^{-1}(U)$ and a finite set.*

REMARK 2.2 (Cyclotomic-dependent points) Since such birational isomorphisms ρ corresponding to characters in the set $\Phi_{X,\mathrm{c}}$ are defined over K_{c}, it is easy to see that for any $\varphi \in \Phi_{X,\mathrm{c}}$, we have $\varphi_X^{-1}(U) \subseteq X(K_{\mathrm{c}})$. So, the set of dependent points in $X(K_{\mathrm{c}})$ is also the union of the set $\bigcup_{\varphi \in \Phi_{X,\mathrm{c}}} \varphi_X^{-1}(U)$ and a finite set.

Taking into account Remark 2.2 we immediately derive:

COROLLARY 2.3 *Under the conditions of Theorem 2.1, the set of dependent points in $X(K_{\mathrm{ab}})$ is the union of a finite set with the set of dependent points in $X(K_{\mathrm{c}})$.*

REMARK 2.4 (Curves of positive genus) Note that if $\Phi_{X,\mathrm{c}}$ is empty, Theorem 2.1 implies that the set of dependent points in $X(K_{\mathrm{ab}})$ is finite. For instance, this automatically occurs if X has genus $g_X > 0$. Indeed, to see this, it is enough to notice that $\mathbb{G}_{\mathrm{m}}$ cannot be birationally isomorphic to X when $g_X > 0$ (by comparing the automorphism groups of $\mathbb{G}_{\mathrm{m}}$ (which is infinite) and of X (which is finite)). However, even if $g_X = 0$, for $\Phi_{X,\mathrm{c}}$ to be non-empty we need the severe condition that some monomial in the coordinate functions on X is a power of a rational function on X of degree 1.

REMARK 2.5 (Elliptic curves with complex multiplication) Let E be an elliptic curve defined by an affine Weierstrass equation over K which has complex multiplication. Without loss of generality, we can assume that K contains the endomorphism ring of E. Then, it is well known that (see, for instance, [**14**]) the field generated over K by all the E-torsion points (that is, torsion points in the sense of elliptic curves) is contained in K_{ab}. So, from Remark 2.4, we know that there are only finitely many E-torsion points which are also dependent.

REMARK 2.6 (Tightness of the assumptions) The assumption of Theorem 2.1 that X is not contained in any translate of a proper algebraic subgroup cannot be replaced with the weaker (obviously necessary) one that X is not contained in any proper algebraic subgroup. This is shown for instance by the example

$$X = \{(x_1, x_2, x_3) \in \mathbb{G}_{\mathrm{m}}^3 \colon x_1 = 2,\ x_3^2 = x_2^3 + 1\}.$$

Then, X has genus 1 (so $\Phi_{X,\mathrm{c}}$ is empty), whereas the infinitely many points $(2, 2^m, \sqrt{2^{3m} + 1}) \in X(\mathbb{Q}_{\mathrm{c}})$, $m \in \mathbb{Z}$, are clearly dependent; also, it is very easy to check that X is not contained in any proper algebraic subgroup. Here, $\sqrt{2^{3m} + 1} \in \mathbb{Q}_{\mathrm{c}}$ due to the Kronecker–Weber theorem.

REMARK 2.7 (Effectiveness) The proof in Section 3 below shows that if X is given effectively, then $\Phi_{X,\mathrm{c}}$ and the finite set appearing in Theorem 2.1 may be effectively computed.

REMARK 2.8 (Non-triviality of isogenies) In general, the isogeny mentioned in the definition of $\Phi_{X,\mathrm{c}}$ cannot be taken trivial. This is equivalent to saying that $\Phi_{X,\mathrm{c}}$ cannot be generally replaced with the set of characters whose restriction to X induces a birational isomorphism $X \cong \mathbb{G}_{\mathrm{m}}$. For an explicit case, see the following Example 1.

EXAMPLE 1 Let X be defined in $\mathbb{G}_{\mathrm{m}}^2$ by $x_1 = (x_2 - 1)^d$. One can check that $\Phi_{X,\mathrm{c}}$ consists of the characters $x_1^{\pm 1}$, $x_2^{\pm 1}$. Note that setting $x_1 = \zeta$, a root of unity, indeed yields the cyclotomic-dependent points $(\zeta, \mu + 1)$ on X, where $\mu^d = \zeta$. Similarly, we may set $x_2 = \zeta$ and get $((\zeta - 1)^d, \zeta)$. For any number field K, Theorem 2.1 implies that these families of points account for all but finitely many dependent points in $X(K_{\mathrm{c}})$. In particular, we recover that equations of the shape $x^m(x - 1)^n = 1$ cannot 'generally' be solved within K_{c}.

One can also supplement Theorem 2.1 with even more explicit descriptions of the dependent points, which would follow as corollaries of its statement (and partially of its proof). In turn, this may lead to other consequences. Here, we do not pursue in this task and limit to the natural question whether a dependence relation $\xi_1^{a_1} \cdots \xi_n^{a_n} = 1$ for $P = (\xi_1, \ldots, \xi_n) \in X(\overline{\mathbb{Q}})$ can be *primitive*, that is, with coprime exponents $\gcd(a_1, \ldots, a_n) = 1$. We say that the corresponding point P is *primitively dependent*.

In fact, the set of primitively dependent points on X is nothing else than the intersection of X with the *union of connected proper algebraic subgroups of* $\mathbb{G}_{\mathrm{m}}^n$.

We need to recall the notion of a field with the Bogomolov Property, see [**2**]:

DEFINITION 2.9 We say that a subfield L of $\overline{\mathbb{Q}}$ has the *Bogomolov Property* if there exists a constant $C(L) > 0$ which depends only on L, such that for any $\alpha \in L^* \backslash U$ we have $\mathrm{h}(\alpha) \geq C(L)$.

For example, in view of [**3**], we can choose $L = K_{\mathrm{c}}$, or even $L = K_{\mathrm{ab}}$, see [**2**] for further examples.

Then we have the following:

THEOREM 2.10 *Under the assumptions of Theorem 2.1 on X, if L is a field with the Bogomolov Property over K, then there are only finitely many primitively dependent points in $X(L)$.*

The same example as in Remark 2.6 shows that again the assumptions on X cannot be weakened. Also, it is easy to see that the set of primitively dependent points in $X(\overline{\mathbb{Q}})$ is always infinite.

As an analogue of Remark 2.5, we record the following remark.

REMARK 2.11 (Elliptic curves) Let E be an elliptic curve defined by an affine Weierstrass equation over $\mathbb{Q}$. By a result of Habegger [8, Theorem 1], the field generated over $\mathbb{Q}$ by all the E-torsion points satisfies the Bogomolov Property. So, it follows from Theorem 2.10 that there are only finitely many E-torsion points which are also primitively dependent.

3. Proofs

3.1. *Notation*

We also recall that the notation $A \ll B$ (sometimes we write this also as $B \gg A$) is equivalent to the inequality $|A| \leq cB$ for some constant c, which throughout the paper may depend on K and X.

3.2. *Proof of Theorem 2.1*

We divide the proof into three steps. We first show that Φ_X is finite, which is our *Step (I)*, and then we prove the second assertion. From Remark 2.2, we know that the set $\bigcup_{\varphi\in\Phi_{X,c}} \varphi_X^{-1}(U)$ is contained in $X(K_{\mathrm{ab}})$ and its elements are dependent points. Besides, any dependent point in $X(K_{\mathrm{ab}})$ is, by definition, mapped to a root of unity under some character φ of $\mathbb{G}_{\mathrm{m}}^n$. So, for the second assertion, we only need to prove that there are only finitely many choices of such a character φ, which we do at *Step* (*II*), and if there are infinitely many points in $X(K_{\mathrm{ab}})$ sent to a root of unity by φ, then $\varphi \in \Phi_{X,\mathrm{c}}$, which is done at *Step* (*III*).

Step (*I*): Proving the finiteness of Φ_X.

Let $\widetilde{X}$ be a smooth projective curve defined over K and K-birational to X. For a character φ, the restriction φ_X to X is a rational function on X, so it is also a rational function on $\widetilde{X}$, and we may consider its divisor $\mathrm{div}(\varphi_X)$ in the set of divisors $\mathrm{Div}(\widetilde{X})$ of $\widetilde{X}$, see [4, Appendix A] for a background on divisors.

We then have a map (a homomorphism) $\varphi \mapsto \mathrm{div}(\varphi_X) \in \mathrm{Div}(\widetilde{X})$ which associates to a (rational) character $\varphi\colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}$ the divisor in $\widetilde{X}$ of φ_X. Note that this map is injective, since any φ in the kernel yields a constant φ_X, which cannot happen in virtue of our assumption on X. Then, it suffices to show that the image of this map on Φ_X is finite.

Let $\varphi \in \Phi_X$, so we may write $\varphi_X \circ \rho(t) = t^d$, where $\rho\colon \mathbb{G}_{\mathrm{m}} \to X$ is a birational isomorphism and t is a coordinate on $\mathbb{G}_m$. In fact, we may extend ρ to an isomorphism $\rho\colon \mathbb{P}_1 \to \widetilde{X}$, and the same equation holds on viewing φ_X as a map from $\widetilde{X}$ to the projective line $\mathbb{P}_1$. Hence, it appears that φ_X can have only one zero and one pole, and so its divisor is of the shape $m((P) - (Q))$ for P, Q distinct points on $\widetilde{X}$. But since φ is a monomial in the coordinates, these P, Q necessarily lie among the zeros and poles of the coordinate functions $x_1, \ldots, x_n$ viewed as functions on $\widetilde{X}$, so P, Q have only finitely many possibilities.

Finally, for given P, Q, let φ, $\psi \in \Phi_X$ correspond to P, Q, such that

$$\mathrm{div}(\varphi_X) = \ell((P) - (Q)) \qquad \text{and} \qquad \mathrm{div}(\psi_X) = m((P) - (Q))$$

for integers ℓ and m. Then $\mathrm{div}((\varphi^m/\psi^\ell)_X) = 0$, so in fact $\varphi^m = \psi^\ell$ by the above injectivity. But both φ, ψ are primitive and this yields $\ell = \pm m$. Hence, each pair P, Q can give rise to at most two elements of Φ_X, and, combined with already established finiteness of the choices for P and Q, the finiteness of Φ_X follows.

Step (*II*): Describing the characters.

To go ahead, we start with some arguments similar to those for [**5**, Theorem 2] (see also [**16**, Chapter 2]).

Let $P \in X(K_{\mathrm{ab}})$ be a dependent point, so the coordinates $\xi_i = x_i(P)$ generate a multiplicative subgroup $\Gamma_P \subset (K_{\mathrm{ab}})^*$ of rank $r \leq n-1$. We may thus write (on invoking elementary abelian group decomposition)

$$\xi_i = \zeta_i \prod_{j=1}^{r} g_j^{m_{ij}}, \qquad i = 1, \ldots, n, \tag{3.1}$$

for generators $g_i \in \mathbb{Q}(P)$ of the torsion-free part of Γ_P, integers m_{ij} and roots of unity $\zeta_i \in \mathbb{Q}(P)$.

Now, by an argument coming from the geometry of numbers, we may actually find the generators g_i so that, for any integers $b_1, \ldots, b_r$,

$$\mathrm{h}(g_1^{b_1} \cdots g_r^{b_r}) \geq c_r(|b_1|\mathrm{h}(g_1) + \cdots + |b_r|\mathrm{h}(g_r)), \tag{3.2}$$

where $c_r > 0$ is a positive number depending only on r; see [**5**, Lemma 2] (which in turn refers to a previous result of Schlickewei [**13**]).

Now, by the already mentioned [**5**, Theorem 1], the height of dependent points in $X(\overline{\mathbb{Q}})$ is uniformly bounded, so that

$$\mathrm{h}\left(\prod_{j=1}^{r} g_j^{m_{ij}}\right) \ll 1.$$

Using then the inequality (3.2) to bound below the height of ξ_i in (1), we find

$$\sum_{j=1}^{r} |m_{ij}|\mathrm{h}(g_j) \ll 1, \tag{3.3}$$

where the implicit constant depends only on X and the ambient dimension n.

In [**5**], this kind of inequality is exploited with $r \leq n-2$ on using certain lower bounds for heights coming from a higher-dimensional version of lower bounds of Dobrowoski, due to Amoroso and David [**1**]. Here we may well have $r = n-1$; however, we may take advantage of the fact that the g_i are in K_{ab} (and certainly they are not roots of unity since they are multiplicatively independent). For these fields, an absolute lower bound for the height has been proved by Amoroso and Zannier [**3**]. Specifically, by [**3**, Theorem 1.2], applied with $\alpha = g_j$, we have

$$\mathrm{h}(g_j) \gg 1, \tag{3.4}$$

where now the implicit constant depends only on K (in fact only on the degree $[K\colon \mathbb{Q}]$). So, here we indeed need that the point P is defined over K_{ab} (the other place we need this is in the end of *Step* (*III*) below).

Combining (3.3) with (3.4), we obtain that the absolute values $|m_{ij}|$ are upper bounded independently of any dependent point $P \in X(K_{\mathrm{ab}})$. We may now consider separately the finitely many

possibilities which arise for the m_{ij}, and thus in the sequel, we may suppose that the m_{ij} are fixed, that is, independent of P.

Let now $(b_1,\dots,b_n)\in\mathbb{Z}^n$ be a non-zero integer vector orthogonal to the $(m_{1j},\dots,m_{nj})$, $j=1,\dots,r$. Since $r<n$, such an integer vector exists, and we may view it as fixed, like for the integers m_{ij}; we may also take it primitive (that is, with coprime coordinates). The previous equations (3.1) for $\xi_1,\dots,\xi_n$ yield

$$\xi_1^{b_1}\cdots\xi_n^{b_n}=\zeta_P, \tag{3.5}$$

where ζ_P is a root of unity (which depends on P). Let us denote by

$$\pi\colon \mathbf{x}\mapsto\mathbf{x}^{\mathbf{b}}$$

the character so obtained, which is primitive in our above meaning.

Note that this character π is taken from a prescribed finite set, and it sends the point P to a root of unity; in fact, this is already an approach to Theorem 2.1. What is missing are the properties of the character stated in Theorem 2.1. So, to complete the proof, we only need to show that if infinitely many points $P\in X(K_{\mathrm{ab}})$ are sent to a root of unity by π, then π is in $\Phi_{X,\mathrm{c}}$.

Step (III): Proving that $\pi\in\Phi_{X,\mathrm{c}}$.

For this, we use [**15**, Theorem 2.1] (we note that in the case of $X(K_{\mathrm{c}})$ the result of [**6**, Theorem 1] is also sufficient).

Let T_k be the set of torsion points of $\mathbb{G}_{\mathrm{m}}^k$, $k\geq 1$. For a rational map τ from a geometrically irreducible variety Y to $\mathbb{G}_{\mathrm{m}}^k$, the (PB) condition in [**15**] means that for any integer $m>0$, the pullback $\mathbb{G}_{\mathrm{m}}^k\times_{[m],\tau}Y$ is geometrically irreducible, where $[m]$ is the mth power map. The result in [**15**, Theorem 2.1] asserts that

> *if τ is a cover (that is, dominant rational map of finite degree) defined over K_{c} and satisfies the* (PB) *condition, there exists a finite union W of proper torsion cosets such that if $v\in T_k\setminus W$, then $v\in\tau(Y)$ and if $\tau(u)=v$, then $[K_{\mathrm{c}}(u)\colon K_{\mathrm{c}}]=\deg\tau$.* (3.6)

So, in order to apply (3.6), we need to construct a suitable cover τ related to the character π. For this, we first factor π_X according to [**15**, Proposition 2.1] into an isogeny of algebraic groups and a rational map satisfying the (PB) condition, from which we can construct a suitable cover. Then, we choose a point u such that we can compute the degree $[K_{\mathrm{c}}(u)\colon K_{\mathrm{c}}]$ from two different ways (including (3.6)) and yield that $\deg\tau=1$ and so τ is an isomorphism, which leads to $\pi\in\Phi_{X,\mathrm{c}}$.

We first show that π_X is a cover. In equation (3.5), fixing a root of unity for the right-hand side gives a proper algebraic subgroup H of $\mathbb{G}_{\mathrm{m}}^n$. Since $X\cap H$ is finite and there are infinitely many $P\in X(K_{\mathrm{ab}})$ such that $\pi_X(P)$ is a root of unity, we must have that $U\cap\pi_X(X(K_{\mathrm{ab}}))$ is infinite, and thus it is Zariski dense in $\mathbb{G}_{\mathrm{m}}$ because obviously (by the finiteness of the roots of a non-trivial univariate polynomial) any closed subset in $\mathbb{G}_{\mathrm{m}}$ is either finite or is $\mathbb{G}_{\mathrm{m}}$ itself. Hence, $\pi_X\colon X\to\mathbb{G}_{\mathrm{m}}$ is a cover.

We can now factor π_X as $\lambda_0\circ\rho_0$ according to the second claim of [**15**, Proposition 2.1] such that $\lambda_0\colon Y\to\mathbb{G}_{\mathrm{m}}$ is an isogeny of algebraic groups and $\rho_0\colon X\to Y$ is a rational map satisfying the (PB) condition. Note that here $(X,Y,\mathbb{G}_{\mathrm{m}})$ correspond to (Y,Z,X) in the notation of

[**15**, Proposition 2.1]. Since there is a dual isogeny $\widehat{\lambda_0}\colon \mathbb{G}_{\mathrm{m}} \to Y$ of λ_0, we see that Y is isomorphic to a quotient of $\mathbb{G}_{\mathrm{m}}$ by a finite subgroup. Now note that a finite subgroup of $\mathbb{G}_{\mathrm{m}}$ is in fact a subgroup of roots of unity. So, it is a kernel of an mth power map $[m]\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$, that is,

$$[m]\colon x \mapsto x^m, \tag{3.7}$$

for some integer $m \geq 1$. Under the power map, we can see that $\mathbb{G}_{\mathrm{m}}$ modulo the kernel (that is, the finite subgroup) is isomorphic to $\mathbb{G}_{\mathrm{m}}$. Therefore, Y is in fact isomorphic to $\mathbb{G}_{\mathrm{m}}$ as algebraic groups. Hence, we in fact can factor

$$\pi_X = [m] \circ \rho, \tag{3.8}$$

where $\rho\colon X \to \mathbb{G}_{\mathrm{m}}$ is a rational map satisfying the (PB) condition, and the mth power map $[m]\colon \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$ is given by (3.7) (see [**4**, Proposition 3.2.17]). Since there are only finitely many such characters π (and also π_X), and so there are only finitely many such integers m, we add all mth roots of unity into K. In other words, we enlarge the field K by adding finitely many roots of unity. Since π and $[m]$ are defined over $\mathbb{Q}$, by (3.8) we know that ρ is defined over K (alternatively, over K_{c} if we do not enlarge the field K).

Furthermore, for any point $P \in X(K_{\mathrm{ab}})$ and any Galois automorphism σ over K, denoting by P^σ the image of P under σ, by definition, we have

$$\rho(P^\sigma) = \rho(P)^\sigma. \tag{3.9}$$

Since π_X is a cover, the map ρ is also a cover. Indeed, if ρ is not a cover, then by definition the image of ρ is not dense in $\mathbb{G}_{\mathrm{m}}$, which by (3.8) implies that the image of π_X is not dense either, contradicting to the fact that π_X is a cover. Now, we define the product cover

$$\psi = \rho \times \rho\colon X \times X \to \mathbb{G}_{\mathrm{m}}^2 \cong \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}},$$

which is also defined over K. Since the cover ρ satisfies the (PB) condition, the same is true for the cover ψ. Clearly, we have $\deg \psi = (\deg \rho)^2$. The cover ψ is exactly what we want for invoking (3.6). The rest is to choose a suitable point.

Since X is defined over K, if $P \in X(K_{\mathrm{ab}})$, then $P^\sigma \in X(K_{\mathrm{ab}})$ for any Galois automorphism σ over K. Note that for any point $P \in X(K_{\mathrm{ab}})$, by (3.8), $\pi_X(P)$ is a root of unity if and only if $\rho(P)$ is a root of unity. So, in view of the infinity of $U \cap \pi_X(X(K_{\mathrm{ab}}))$, we know that $U \cap \rho(X(K_{\mathrm{ab}}))$ is also infinite. Thus, considering the set S of images of points of the form (P, P^σ) under ψ for any $P \in \rho^{-1}(U) \cap X(K_{\mathrm{ab}})$ and any Galois automorphism σ over K, S is an infinite set and is a torsion subset of $\mathbb{G}_{\mathrm{m}}^2$, whose elements by (3.9) have the form (ζ, ζ^σ) for some root of unity ζ. Applying (3.6) to both ρ and ψ and noticing that each proper torsion coset of $\mathbb{G}_{\mathrm{m}}^2$ contains only finitely many torsion points of such form (ζ, ζ^σ), there exist an element $(\zeta, \zeta^\sigma) \in S$ and a point (P, P^σ) with $P \in X(K_{\mathrm{ab}})$ mapped to (ζ, ζ^σ) under ψ such that

$$[K(P)\colon K] = \deg \rho, \qquad [K(P, P^\sigma)\colon K] = \deg \psi = (\deg \rho)^2.$$

On the other hand, since $P \in X(K_{\mathrm{ab}})$, the field extension $K(P)/K$ is automatically normal, whence it contains $K(P^\sigma)$ for any conjugate P^σ of P over K. So, we obtain

$$[K(P, P^{\sigma}): K] = [K(P): K] = \deg \rho.$$

Hence, we must have $\deg\rho = 1$. That is, ρ is an isomorphism. So, by (3.8), we have $\pi_X \circ \rho^{-1} = [m]$, which is an isogeny of $\mathbb{G}_{\mathrm{m}}$, and thus $\pi \in \Phi_{X,\mathrm{c}}$. This completes the proof.

3.3. *Proof of Theorem 2.10*

Let $P = (\xi_1, \dots, \xi_n) \in X(L)$ be a primitively dependent point, and let $\xi_1^{a_1} \cdots \xi_n^{a_n} = 1$ be a primitive relation, that is, with the a_i coprime integers.

We could indeed use the result of Theorem 2.1 for the proof if $L = K_{\mathrm{ab}}$, but it is as easy to go again through the proof. Arguing exactly as in the previous proof (equation (3.4) still holds since L has the Bogomolov Property), we find bounded integers m_{ij}, $1 \le i \le n$, $1 \le j \le r$, and generators g_j for the group $\xi_1^{\mathbb{Z}} \cdots \xi_n^{\mathbb{Z}}$ as above. Here r is again the rank of such group. It follows that the vectors $(m_{1j}, \dots, m_{nj})$, $j = 1, \dots, r$, are linearly independent.

Note that $(a_1, \dots, a_n)$ must be orthogonal to the $(m_{1j}, \dots, m_{nj})$, $j = 1, \dots, r$, by the independence of the g_j.

If $r = n - 1$, then the space orthogonal to the $(m_{1j}, \dots, m_{nj})$, $j = 1, \dots, r$, has dimension 1, hence $(a_1, \dots, a_n)$ is uniquely determined up to sign, since it is primitive. Hence, since the m_{ij} are bounded, it has only finitely many possibilities, and the equation $x_1^{a_1} \cdots x_n^{a_n} = 1$ yields only finitely many points $P \in X$.

Therefore, we may assume that $r \le n - 2$. Now, we could conclude immediately by using [5, Theorem 2], which yields finiteness for points verifying two or more independent multiplicative relations. But we can conclude in an easier way, without using such result.

For this, let us start by observing that a standard argument yields two independent vectors

$$(b_1, \dots, b_n) \qquad \text{and} \qquad (c_1, \dots, c_n)$$

orthogonal to the vectors $(m_{1j}, \dots, m_{nj})$, $j = 1, \dots, r$, and bounded independently of P (since the m_{ij} are likewise bounded). Hence, we may assume that these vectors are fixed for an infinity of the points P in question.

Let φ, ψ be the corresponding characters, which are multiplicatively independent. Then, $\varphi(P)$ and $\psi(P)$ are both roots of unity. The map $(\varphi, \psi)\colon \mathbb{G}_{\mathrm{m}}^n \to \mathbb{G}_{\mathrm{m}}^2$ is a homomorphism sending the curve X to a curve $Y \subset \mathbb{G}_{\mathrm{m}}^2$. The curve Y then contains the torsion points $(\varphi(P), \psi(P))$. If these points make up an infinite set, then Y is a translate of a torus. But then, by the multiplicative independence of φ and ψ, X is contained in a non-trivial translate of an algebraic subgroup, against the assumptions. Hence, there are only finitely many points $\varphi(P)$, which then implies that P lies in a finite set.

4. Possible generalizations and applications

Remark 4.1 (Higher dimensions) One may ask what happens for higher dimensional varieties in place of the curve X. Now the bounded-height result of [5], which is a crucial tool for the present proofs, is not true in the most obvious generalization, but a correct analogue has been proved by Habegger [7]. Probably this leads to higher-dimensional analogues of the present conclusions.

REMARK 4.2 (Multiplicative dependence of rational values) We recall that any n rational functions over K in one variable t, not all constant, always parametrize a curve X, which is rational over K. Hence, our results can be used to investigate multiplicative dependence of the values on K_c (or more generally on K_{ab}) of given rational functions in $K(t)$. To satisfy the necessary condition of Theorem 2.1, we have to make a natural assumption that there is no non-trivial product of these rational functions which is a constant function. We refer to [**11**] for some partial results.

Acknowledgement

The authors would like to thank the referee for giving constructive comments which helped to improve the paper.

Funding

During the preparation of this work, A.O. was supported by the UNSW FRG Grant PS43704, M.S. was supported by the Macquarie University Research Fellowship, and I.S. was supported by the ARC Grant DP170100786.

References

1. F. Amoroso and S. David, Le probléme de Lehmer en dimension suplérieure, *J. Reine Angew. Math.* **513** (1999), 145–179.
2. F. Amoroso, S. David and U. Zannier, On fields with Property (B), *Proc. Amer. Math. Soc.* **142** (2014), 1893–1910.
3. F. Amoroso and U. Zannier, A uniform relative Dobrowolski's lower bound over abelian extensions, *Bull. Lond. Math. Soc.* **42** (2010), 489–498.
4. E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge University Press, Cambridge, 2006.
5. E. Bombieri, D. Masser and U. Zannier, Intersecting a curve with algebraic subgroups of multiplicative groups, *Int. Math. Res. Notices* **1999** (1999), 1119–1140.
6. R. Dvornicich and U. Zannier, Cyclotomic Diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps), *Duke Math. J.* **139** (2007), 527–554.
7. P. Habegger, On the bounded height conjecture, *Int. Math. Res. Notices* **2009** (2009), 860–886.
8. P. Habegger, Small height and infinite nonabelian extensions, *Duke Math. J.* **162** (2013), 2027–2076.
9. S. Lang, Division points on curves, *Ann. Mat. Pura Appl.* **70** (1965), 229–234.
10. M. Laurent, Equations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299–327.
11. A. Ostafe, M. Sha, I. E. Shparlinski and U. Zannier, *On multiplicative dependence of values of rational functions*, Preprint, 2017, https://arxiv.org/abs/1706.05874.
12. P. Sarnak and S. Adams, Betti numbers of congruence groups, *Israel J. Math.* **88** (1994), 31–72, with an appendix by Z. Rudnick.
13. H. P. Schlickewei, Lower bounds for heights on finitely generated groups, *Monatsh. Math.* **123** (1997), 171–178.

14. J.-P. Serre, Complex Multiplication, *Algebraic Number Theory* (Eds. J. W. S. Cassels and A. Fröhlich), Academic Press, London, 1967, 292–296.
15. U. Zannier, Hilbert irreducibility above algebraic groups, *Duke Math. J.* **153** (2010), 397–425.
16. U. Zannier, Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Annals of Mathematical Studies, Vol. 181*, Princeton University Press, Princeton, NJ, 2012.
17. U. Zannier, Lecture notes on Diophantine analysis, Publ. Scuola Normale Superiore, Pisa, 2014.