IMRN International Mathematics Research Notices
1999, No. 20

Intersecting a Curve with Algebraic Subgroups of Multiplicative Groups

E. Bombieri, D. Masser, and U. Zannier

§1 Introduction and results

The results of this paper originated from the following question: What can be said about the set of algebraic numbers $\tau \neq 0, 1$ for which τ and $1-\tau$ are multiplicatively dependent? It is easy to see that this set is infinite. On the other hand, simple arguments show that its restriction to the rational integers $\mathbb{Z}$ is $\{-1, 2\}$ and its restriction to the rational numbers $\mathbb{Q}$ is $\{-1, 1/2, 2\}$. If one considers the restriction to a number field F, then by looking at $x^a(1-x)^b = 1$ with a, b modulo a large integer N, one is led to rational points in F on the curve $x^r(1-x)^s = y^N$, and Faltings's theorem suffices to deal with this if the curve has genus at least 2. However, this approach leads to difficulties if the curve has genus 0 or 1. Finally, if one considers the restriction to the set of algebraic numbers of fixed degree, then specialization estimates (see Masser [Ma]) show that this restriction must be a very sparse set.

Our Theorem 1 below improves all these observations and, in particular, implies that the sparse set alluded to is actually finite. Furthermore, it shows that the original unrestricted set is a set of bounded Weil height in the algebraic numbers $\overline{\mathbb{Q}}$, which is even stronger in view of the well-known Northcott finiteness theorem.

There is nothing special about $x^a(1-x)^b = 1$, which may be thought of as the intersection of the curve $x+y = 1$ sitting inside $\mathbb{G}_m^2 = \{xy \neq 0\}$ with the variable algebraic subgroup $x^a y^b = 1$ of $\mathbb{G}_m^2$. Hence the first question we ask is about the intersection of a curve C in $\mathbb{G}_m^n$ with the family of proper algebraic subgroups of $\mathbb{G}_m^n$.

Received 7 May 1999. Revision received 15 August 1999.

By a torus, we mean a connected algebraic subgroup of $\mathbb{G}_m^n$. In what follows, we use the height on $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ defined by

$$h\big((x_1,\dots,x_n)\big) = h(x_1) + \cdots + h(x_n),$$

where $h(x)$ is Weil's absolute logarithmic height. Our first result is the following.

Theorem 1. Let C be a closed absolutely irreducible curve in $\mathbb{G}_m^n$, $n \geq 2$, defined over $\overline{\mathbb{Q}}$ and not contained in a translate of a proper subtorus of $\mathbb{G}_m^n$.

Then the points of $C \cap H(\overline{\mathbb{Q}})$ for H ranging over all proper algebraic subgroups of $\mathbb{G}_m^n$ form a set of bounded Weil height. □

Remark. For the original problem with x and $1-x$, Paula Cohen and the third author [CZ] have found the best possible bound $\log 2$ for the height and have shown that it is isolated, in the sense that for $x \neq 1/2, 2$, the height does not exceed $\log 2 - \delta$ for an absolute constant $\delta > 0$.

Remark. The condition that C is not contained in a translate of a proper subtorus is necessary for the validity of the theorem. In fact, suppose $C \subset gH$ with H a proper subtorus of $\mathbb{G}_m^n$. If g is a torsion point, C is contained in a proper subgroup H' of $\mathbb{G}_m^n$; therefore, the set $C \cap H'(\overline{\mathbb{Q}}) = C(\overline{\mathbb{Q}})$ has unbounded height. If instead g is not a torsion point, we proceed as follows. After a monoidal change of coordinates, we may assume that H is the subtorus $x_n = 1$, gH is given by $x_n = g_n$, and x_1 is not a constant function on C. Then the torus H_m given by $x_1 = x_n^m$ has a nonempty intersection with C for infinitely many integers m. Every point $\mathbf{x}$ of $C \cap H_m$ has $x_1 = g_n^m$; hence $h(\mathbf{x}) = \sum h(x_i) \geq (|m|+1)h(g_n)$, which is unbounded as $m \to \infty$.

Remark. If C is absolutely irreducible, defined over $\overline{\mathbb{Q}}$, and not contained in a proper algebraic subgroup of $\mathbb{G}_m^n$, then we have $C \bigcap H(\mathbb{C}) = C \bigcap H(\overline{\mathbb{Q}})$ for any proper algebraic subgroup H of $\mathbb{G}_m^n$. For the proof, it suffices to note that H is defined over $\mathbb{Q}$ and C is defined over a number field.

An equivalent formulation of Theorem 1 is as follows, where the height is now chosen intrinsically on the curve C (see Proposition B below).

Theorem 1′. Let C be an absolutely irreducible curve defined over $\overline{\mathbb{Q}}$, and let $x_1,\dots,x_n$ be nonzero rational functions in $\overline{\mathbb{Q}}(C)$, multiplicatively independent modulo constants. Then the points $P \in C(\overline{\mathbb{Q}})$, for which $x_1(P),\dots,x_n(P)$ are multiplicatively dependent, form a set of bounded Weil height. □

This equivalence can be verified by looking at the rational map $C \to \mathbb{G}_m^n$ given by $P \mapsto (x_1(P),\dots,x_n(P))$ and noting that every proper algebraic subgroup of $\mathbb{G}_m^n$ is

contained in a subgroup $x_1^{a_1} \cdots x_n^{a_n} = 1$. Then the condition that the image of C is not contained in a translate of a subgroup is equivalent to the condition that no nontrivial product $x_1^{a_1} \cdots x_n^{a_n}$ is a constant function.

In this form, Theorem 1′ may be considered as an analogue for $\mathbb{G}_m^n$ of Silverman's specialization theorem for abelian varieties (see [Sil]); or rather the earlier version for "split families" due to Demjanenko [D] and Manin [M] (see our later discussion).

An immediate consequence of Theorem 1′ is that if $\alpha_1, \ldots, \alpha_n$ are distinct elements of $\mathbb{Z}$, then there are only finitely many τ in $\mathbb{Z}$ such that $\tau - \alpha_1, \ldots, \tau - \alpha_n$ are nonzero and multiplicatively dependent. This particular result can be found in an unpublished manuscript of J. Thompson, dating back to 1987.

Theorem 1 refers to algebraic subgroups H of dimension $\dim(H) \leq n - 1$. If we consider the intersection of C with subgroups of dimension at most $n - 2$, then we can prove a more striking result.

Theorem 2. Let $C \subset \mathbb{G}_m^n$ satisfy the assumptions of Theorem 1. Then the points of $C \bigcap H(\mathbb{C})$ for H ranging over all algebraic subgroups of $\mathbb{G}_m^n$ with $\dim(H) \leq n - 2$ form a finite set. □

Theorem 2 admits a formulation analogous to Theorem 1′, which we leave to the reader.

Remark. The special case of intersections with tori of dimension 1 is an easy consequence of Theorem 7 of Schinzel [S].

Remark. We saw that the main condition of Theorem 1 (and Theorem 2), namely, that C is not contained in a translate of some proper subtorus, is necessary for the validity of Theorem 1. It is not quite clear if this condition is also necessary for the validity of Theorem 2. The following discussion may help to put the problem into perspective.

Definitely necessary is the weaker condition that C does not lie in a proper subgroup. So we assume this latter condition but also that C does indeed lie in a translate of some proper subtorus H_0.

Suppose first that $\dim(H_0) = 1$, so that after a monoidal change of coordinates we may assume that C is given by $x_2 = g_2, \ldots, x_n = g_n$ with $g_i \in \overline{Q}^*$. These must be multiplicatively independent, and it follows easily that $C \bigcap H$ is empty whenever $\dim(H) \leq n - 2$. So Theorem 2 does hold in this case.

Next suppose $\dim(H_0) = 2$, and as above we may suppose that C is the curve $f(x_1, x_2) = 0$, $x_3 = g_3, \ldots, x_n = g_n$. Then the study of $C \bigcap H$ amounts to solving the equation $f(x_1, x_2) = 0$ for x_1, x_2 in the division group of the group generated by $g_3, \ldots, g_n$. This is precisely the situation in a well-known result of Liardet (see, for example,

[L, Theorem 7.3, p. 207]), and it is easy to verify that Theorem 2 again follows. A special case is the solution of, say, $2^u - 3^v = 1$, in positive integers u, v. However, the original proof of Liardet's result involves Siegel's theorem, and the resulting bound for the height of x_1, x_2 is not effective unless one brings in other methods.

Now suppose that $\dim(H_0) = 3$, so that we may suppose that C is the curve $f(x_1, x_2, x_3) = g(x_1, x_2, x_3) = 0$, $x_4 = g_4, \dots, x_n = g_n$. Then Liardet's theorem seems insufficient, and the problem appears to be of a new kind. For example, What is the nature of the set of algebraic numbers τ such that there are at least two independent multiplicative relations between 2, 3, τ, $1-\tau$, and $1+\tau$? This includes the solution of $2^u - 3^v = 1$ as well as the problem solved in [CZ], namely, the determination of all algebraic numbers τ not 0, 1 or -1 such that there are two independent multiplicative relations between τ, $1-\tau$, and $1+\tau$. There are 34 such numbers, namely, *the 12-th roots of unity excluding* ± 1 *and the solutions of the relations* $x^{-6}(x-1)^6(x+1)^6 = 1$, $x^2(x-1)^2(x+1)^2 = 1$ *and* $x^{-6}(x-1)^2(x+1)^2 = 1$.

In the special case in which H has dimension 0, Theorem 2 states that C contains only finitely many torsion points. Many simple proofs are known of this particular result, which is also a special case of the aforementioned result of Liardet. This is the $\mathbb{G}_m^n$ analogue of a much deeper conjecture of Manin and Mumford on abelian varieties, proved by Raynaud in [R]. However, as far as we know, no direct analogue of Theorem 2 for abelian varieties appears in the literature. One such possible extension could deal with the intersection of a curve C in an abelian variety A with the family of all proper algebraic subgroups in A, reducing to Raynaud's theorem if A is simple. Another extension (as in [Sil]) could consider a family $\mathcal{A} \to C$ with general fiber an abelian variety, using sections in place of rational functions. This generalization is meaningless for a multiplicative group because the map always splits after a finite base change ($\mathbb{G}_m^n$ has no moduli), but the abelian variety case could lead to new, interesting features.

The extension of our results, and of possible analogues for abelian varieties, to the case of a general subvariety X of a commutative algebraic group is also an interesting problem. The case of the intersection of $X \subset \mathbb{G}_m^n$ with subgroups of dimension 1 can be treated by methods similar to those introduced here, and will be the subject of a future paper.

Here is a short description of our methods and of the arrangement of this paper.

Section 2 begins with a direct proof of Theorem 1′ for C a curve of genus 0, yielding a completely explicit result. The proof in the general case is along similar lines and based on a refinement (Proposition B′) of a well-known result about heights on a curve induced by rational functions. The proof of this refinement depends on a lemma (Lemma 1) that may be of independent interest.

Section 3 gives a new proof of Theorem 1 using tools from geometry of numbers. Lemma 2, which may be useful in other situations, states the existence of good generators in finitely generated subgroups of $\overline{\mathbb{Q}}^*$, such that the Weil height becomes quasi-additive with respect to these generators.

Section 4 proceeds with the proof of Theorem 2. Again, Lemma 2 and geometry of numbers play an important role, but in addition, we need a very recent result of Amoroso and David, extending a well-known lower bound of Dobrowolski for the height of algebraic numbers to the case of heights in a finitely generated subgroup of $\overline{\mathbb{Q}}^*$. The use of Dobrowolski's estimate in a not unrelated context is also in Schinzel's paper [S].

Dobrowolski's estimate alone suffices to deal with the case in which we consider the intersection of C with subgroups of dimension less than $(n-1)/2$, and the full result of Amoroso and David easily suffices for the intersection with subgroups of dimension at most $n-3$.

This argument just fails in the most interesting case of the intersection with subgroups of dimension $n-2$. The proof is completed with a further application of the Amoroso–David result (Lemma 4) and an intricate argument from algebraic number theory (Lemmas 5 and 6), with a definite cohomological flavour.

We conclude with the remark that all our results are in principle effective, but we have made no attempt here to obtain explicit constants except in the first part of Section 2.

§2 Proof of Theorem 1

We begin by proving Theorem 1 in the special but significant case in which $C = \mathbb{P}^1$. We start with the following proposition.

Proposition A. Let $\mathcal{A}$ be a set of s distinct algebraic numbers of height at most A, $A \geq \log 2$. Let

$$x(t) = \prod_{\alpha \in \mathcal{A}} (t-\alpha)^{e_\alpha}$$

be a rational function of t whose zeros and poles are supported in the set $\mathcal{A} \cup \infty$. Then for every $\tau \in \overline{\mathbb{Q}}$, τ not a zero or pole of x, we have

$$-(s+1)^2 A \cdot \deg(x) \leq h\big(x(\tau)\big) - \deg(x)h(\tau) \leq (s+1)A \cdot \deg(x). \qquad \square$$

Remark. The boundedness of $h(x(\tau)) - \deg(x)h(\tau)$ as a function of τ is a well-known consequence of the functorial properties of the height. The point of Proposition A is that

this bound is actually linear in $\deg(x)$ for fixed $\mathcal{A}$, which is optimal. However, we do not claim that the constants given here, in particular the quadratic dependence on $s+1$ in the lower bound, are optimal in any way.

Proof. Let $\mathcal{B}$ and $\mathcal{C}$ be the sets of finite zeros and poles of the rational function x. We write

$$x(t) = \frac{P(t)}{Q(t)} = \frac{\prod_{\beta\in\mathcal{B}}(t-\beta)^{e_\beta}}{\prod_{\gamma\in\mathcal{C}}(t-\gamma)^{e_\gamma}}$$

with $e_\beta, e_\gamma > 0$, and write for simplicity $d = \sum_{\mathcal{B}} e_\beta$, $d' = \sum_{\mathcal{C}} e_\gamma$, so that $\deg(x) = \max(d, d')$.

In order to compute the height, let k be a number field containing the zeros and poles of x and the algebraic number τ, and denote by $|\quad|_v$ the elements of a full set of normalized absolute values in k so that the product formula in k holds. Then we have

$$\begin{aligned} h\big(x(\tau)\big) &= \sum_v \max\big(\log|P(\tau)|_v, \log|Q(\tau)|_v\big) \\ &= \sum_v \max\left(\sum_{\mathcal{B}} e_\beta \log|\tau-\beta|_v, \sum_{\mathcal{C}} e_\gamma \log|\tau-\gamma|_v\right). \end{aligned} \tag{2.1}$$

We have a general inequality

$$\log|p-q|_v \le \max\big(\log|p|_v, \log|q|_v\big) + \varepsilon_v \log 2, \tag{2.2}$$

where $\varepsilon_v = 0$ if v is finite, and $\varepsilon_v = [k_v : \mathbb{Q}_v]/[k:\mathbb{Q}]$ if v is infinite. If we set $p = \tau$ and $q = \beta$ or $q = \gamma$ in (2.2), we obtain from (2.1) the upper bound

$$\begin{aligned} h\big(x(\tau)\big) &= \sum_v \max\left(\sum_{\mathcal{B}} e_\beta \log|\tau-\beta|_v, \sum_{\mathcal{C}} e_\gamma \log|\tau-\gamma|_v\right) \\ &\le \max(d,d') \sum_v \left\{\varepsilon_v \log 2 + \max_{\mathcal{B},\mathcal{C}} \max\big(\log|\tau|_v, \log|\beta|_v, \log|\gamma|_v\big)\right\} \\ &\le \deg(x)\left(h(\tau) + \sum_{\mathcal{A}} h(\alpha) + \log 2\right). \end{aligned}$$

This proves the right-hand side inequality of Proposition A.

The proof of the lower bound is rather similar. In what follows, we write for simplicity $\log^+ t$ instead of $\max(\log t, 0)$.

We claim first that

$$\max\left(d\log|\tau-\beta|_v, d'\log|\tau-\gamma|_v\right) \geq \max(d,d')\left\{\log^+|\tau|_v - \varepsilon_v\log 4 - \max\left(\log^+|\beta|_v, \log^+|\gamma|_v\right) - \log^+\frac{1}{|\beta-\gamma|_v}\right\}. \tag{2.3}$$

In fact, we may assume $d \geq d'$. Inequality (2.2) with $p = \tau-\beta$, $q = -\beta$ yields

$$\log^+|\tau|_v \leq \log^+|\tau-\beta|_v + \log^+|\beta|_v + \varepsilon_v\log 2, \tag{2.4}$$

and this suffices for proving (2.3) if $\log|\tau-\beta|_v \geq 0$; we just multiply (2.4) by d, and (2.3) follows. If $\log|\tau-\beta|_v < 0$ and $\log|\tau-\gamma|_v \geq 0$, we simply note that the left-hand side of (2.3) is positive or zero and the right-hand side of (2.3) is negative or zero, again because of (2.4). If instead $\log|\tau-\beta|_v < 0$ and $\log|\tau-\gamma|_v < 0$, we note that $d'\log|\tau-\gamma|_v \geq d\log|\tau-\gamma|_v$; and so it suffices to prove (2.3) in the case $d = d'$. In this case, we may further assume that $\log|\tau-\beta|_v \geq \log|\tau-\gamma|_v$. Then we use (2.2) with $p = \tau-\beta$, $q = \tau-\gamma$, obtaining

$$\log|\beta-\gamma|_v \leq \log|\tau-\beta|_v + \varepsilon_v\log 2.$$

We combine this inequality with (2.4) and find

$$\log^+|\tau|_v + \log|\beta-\gamma|_v \leq \log^+|\beta|_v + \varepsilon_v\log 2 + \log|\tau-\beta|_v + \varepsilon_v\log 2,$$

yielding again (2.3) after multiplication by d.

From (2.1) and (2.3), we get

$$\begin{aligned} &h(x(\tau)) \\ &= \sum_v \max\left(\sum_{\mathcal{B}} e_\beta\log|\tau-\beta|_v, \sum_{\mathcal{C}} e_\gamma\log|\tau-\gamma|_v\right) \\ &\geq \sum_v \max\left(d\min_{\mathcal{B}}\log|\tau-\beta|_v, d'\min_{\mathcal{C}}\log|\tau-\gamma|_v\right) \\ &\geq \deg(x)\left\{h(\tau) - \log 4 - \sum_v \max_{\mathcal{B},\mathcal{C}}\left(\max\left(\log^+|\beta|_v, \log^+|\gamma|_v\right) + \log^+\frac{1}{|\beta-\gamma|_v}\right)\right\}. \end{aligned}$$

Finally,

$$\sum_v \max_{\mathcal{B},\mathcal{C}}\left(\max\left(\log^+|\beta|_v, \log^+|\gamma|_v\right) + \log^+\frac{1}{|\beta-\gamma|_v}\right) \leq \sum_{\mathcal{B}} h(\beta) + \sum_{\mathcal{C}} h(\gamma) + \sum_{\mathcal{B}}\sum_{\mathcal{C}} h\left(\frac{1}{\beta-\gamma}\right) \leq sA + \left(\frac{s}{2}\right)^2(2A+\log 2),$$

which combined with the preceding inequality yields

$$h(x(\tau)) \geq \deg(x)h(\tau) - \deg(x)\left(\log 4 + sA + \left(\frac{s}{2}\right)^2 (2A + \log 2)\right).$$

Since we assume $A \geq \log 2$, the left-hand side of the inequality of Proposition A follows with ample margin.

We can now prove Theorem 1′ in the rational case. Let $x = \prod x_i^{b_i}$, with rational integer exponents, not all zero. We want to prove that the points τ for which $x(\tau) = 1$ have uniformly bounded height.

We factorize each rational function $x_i(t)$ as

$$x_i(t) = a_i y_i(t) = a_i \prod_{\alpha \in \mathcal{A}} (t - \alpha)^{e_{\alpha i}}$$

and write

$$x(t) = a y(t), \qquad a = \prod a_i^{b_i}, \qquad y(t) = \prod y_i(t)^{b_i}.$$

Then $y(t) = \prod (t - \alpha)^{e_\alpha}$ with

$$e_\alpha = \sum_i e_{\alpha i} b_i. \tag{2.5}$$

Since by hypothesis, the function $x(t)$ is always a nonconstant function, the matrix with entries $e_{\alpha i}$ has maximal rank, and it follows from (2.5) that

$$\max_\alpha |e_\alpha| \geq c \max_i |b_i|$$

for some constant $c > 0$ depending only on the matrix $e_{\alpha i}$. In particular, we deduce that

$$\deg(y) \geq c \max_i |b_i|. \tag{2.6}$$

Now we apply Proposition A to the function $y(t) = a^{-1}x(t)$ at a point τ for which $x(\tau) = 1$. We find

$$h(a^{-1}) = h(y(\tau)) \geq \deg(y)\{h(\tau) - (s+1)^2 A\},$$

where s is the cardinality of the set $\mathcal{A}$ and $A \geq \log 2$ is an upper bound for the heights of the elements of $\mathcal{A}$. Hence, using (2.6), we get

$$\begin{aligned}\deg(y)h(\tau) &\le \deg(y)(s+1)^2A + h(a^{-1}) \\ &\le \deg(y)(s+1)^2A + \sum_i |b_i| h(a_i) \\ &\le \deg(y)\Big\{(s+1)^2A + c^{-1}\sum_i h(a_i)\Big\}.\end{aligned}$$

If we divide by $\deg(y)$, we obtain the required uniform bound independent of the exponents b_i.

The proof of the general case follows similar lines. We recall the following result on heights. ■

Proposition B. Let $h(P)$, $P \in C(\overline{\mathbb{Q}})$, be a height on C determined by a choice of a divisor[1] of degree 1 on C, and let x be a rational function in $\overline{\mathbb{Q}}(C)$.

Then for $P \in C(\overline{\mathbb{Q}})$ not a zero or pole of x, we have

$$h(x(P)) = \deg(x)h(P) + O\big(1 + \sqrt{h(P)}\big), \tag{2.7}$$

where $h(x(P))$ is the Weil height. Here the constant involved in the O symbol may depend on the rational function x. □

Proof. This is a well-known result due to Néron [N]. A weaker formulation, which goes back to Siegel [Si], is the asymptotic result $\deg(y)h(x(P)) \sim \deg(x)h(y(P))$, valid for any two nonconstant functions x, y on C. This could be used, in our subsequent arguments here and in §3, in place of the more precise Proposition B.

The next result is a uniform version of Proposition B. ■

Proposition B′. Let h be a height on C as before. Let $\mathcal{X}$ be a finitely generated subgroup of $\overline{\mathbb{Q}}(C)^*$, and suppose that the only constant functions in $\mathcal{X}$ are roots of unity.

Then for $x \in \mathcal{X}$ and $P \in C(\overline{\mathbb{Q}})$ not a zero or pole of x, we have

$$h(x(P)) = \deg(x)\Big\{h(P) + O\big(1 + \sqrt{h(P)}\big)\Big\},$$

where the constant involved in the O symbol depends only on the group $\mathcal{X}$. □

Proof. One can obtain a proof by mimicking the proof of Proposition A using Weil functions or Weil's Théorème de Décomposition, as in [B], in order to obviate the absence, for a rational function on C, of the analogue of the factorization of a rational function on $\mathbb{P}^1$ in linear factors. However, it may be of independent interest to notice that Proposition B′ can be deduced directly from estimate (2.7) of Proposition B the following way. ■

[1] Strictly speaking, this height depends also on a choice of a set of Weil functions associated to this divisor.

Definition. Let $\mathcal{X}$ be a finitely generated subgroup of $\overline{\mathbb{Q}}(C)^*$. A noncancelling semigroup $S \subset \mathcal{X}$ is a semigroup generated by finitely many nonconstant elements $x_1, \dots, x_n \in \mathcal{X}$ with the property that no zero of a generator x_i is a pole of another generator x_j.

The main property of noncancelling semigroups is that the degree becomes additive; namely, in a noncancelling semigroup, we have

$$\deg\left(\prod_{i=1}^{n} x_i^{e_i}\right) = \sum_{i=1}^{n} e_i \deg(x_i), \quad e_i \geq 0. \tag{2.8}$$

Let

$$x = \prod_{i=1}^{n} x_i^{e_i}$$

be an element of a noncancelling semigroup and let P be an algebraic point on C, not a zero or pole of x. Then P is also not a zero or pole of any x_i and

$$h\big(x(P)\big) \leq \sum_{i=1}^{n} e_i h\big(x_i(P)\big).$$

In view of (2.7), (2.8), and Proposition B for each function x_i, we deduce

$$\begin{aligned} h\big(x(P)\big) &\leq \sum_{i=1}^{n} e_i h\big(x_i(P)\big) \\ &= \sum_{i=1}^{n} e_i \deg(x_i)\Big\{h(P) + O\big(1 + \sqrt{h(P)}\big)\Big\} \\ &= \deg(x)\Big\{h(P) + O\big(1 + \sqrt{h(P)}\big)\Big\}, \end{aligned}$$

which is half of the conclusion of Proposition B′ with $\mathcal{X}$ replaced by a noncancelling semigroup.

In order to obtain the corresponding lower bound, one applies this upper bound to the element

$$z = x_1^{e-e_1} \cdots x_n^{e-e_n} = y^e x^{-1}$$

of the same semigroup, where now $e = \max e_i$ and $y = x_1 \cdots x_n$. This gives

$$h\big(z(P)\big) \leq \big(e \deg(y) - \deg(x)\big)h(P) + O\big(e + e\sqrt{h(P)}\,\big).$$

Since $y^e(P) = x(P)z(P)$, we also have

$$eh\big(y(P)\big) \le h\big(x(P)\big) + h\big(z(P)\big).$$

Then the lower bound follows easily from the last two displayed inequalities, by applying (2.7) to $y(P)$ and noting that since every x_i is a nonconstant function, we have $\deg(x_i) \ge 1$ and $e \le \sum e_i \deg(x_i) = \deg(x)$.

In order to complete the proof of Proposition B′, we remark that we may assume that $\mathcal{X} \bigcap \overline{\mathbb{Q}} = 1$, since we can argue with $\mathcal{X}^N$ instead of $\mathcal{X}$ and choose N so to kill the torsion. Therefore, once we have proved Proposition B′ for the elements of a noncancelling semigroup, the proof is completed by the following lemma.

Lemma 1. Let $\mathcal{X}$ be a finitely generated subgroup of $\overline{\mathbb{Q}}(C)^*$, and suppose that $\mathcal{X} \bigcap \overline{\mathbb{Q}} = 1$. Then $\mathcal{X}$ is a finite union of noncancelling semigroups. □

Remark. The proof we give below turns out to be quite efficient in practice. For example, if $C = \mathbb{P}^1$ and $\mathcal{X}$ is generated by $x = t$ and $y = 1 - t$, we find that $\mathcal{X}$ breaks into the union of six noncancelling semigroups, each generated by two consecutive functions from the list

$$x, y, \frac{y}{x}, \frac{1}{x}, \frac{1}{y}, \frac{x}{y}, x.$$

Proof. Let $P_1, \dots, P_s$ be the support of the set of zeros and poles of all elements of $\mathcal{X}$. There is a homomorphism m from $\mathcal{X}$ to $\mathbb{Z}^s$ defined by $m(x) = (m_1, \dots, m_s)$, where m_i is the order of zero of x in P_i. Because $\mathcal{X} \bigcap \overline{\mathbb{Q}} = 1$, the homomorphism m is injective, and the image G of $\mathcal{X}$ by m is a subgroup of $\mathbb{Z}^s$, isomorphic to $\mathcal{X}$.

Now let Λ be any region in $\mathbb{R}^s$ defined by inequalities $L \ge 0$ for finitely many linear forms with rational coefficients. It is well known (Gordan's lemma—see, for example, Proposition 1.1(ii) of [O]) that the additive semigroup $G \bigcap \Lambda$ is either 0 or finitely generated. In particular, let $\mathbf{u} = (u_1, \dots, u_s)$ be a vector with components $u_i = \pm 1$, and let $\Lambda_{\mathbf{u}}$ be the orthant of $\mathbb{R}^s$ defined by $u_1 z_1 \ge 0, \dots, u_s z_s \ge 0$. If $G_{\mathbf{u}} = G \bigcap \Lambda_{\mathbf{u}}$ is not 0 and its generators are $m(x_1), \dots, m(x_n)$, it becomes plain that no zero of x_i can be a pole of x_j. Thus $\mathcal{X}$ is the union of the noncancelling semigroups $m^{-1}(G_{\mathbf{u}})$, concluding the proof.

We can now prove Theorem 1′ in general. Let $\mathcal{X}$ be the group generated by the rational functions $x_1, \dots, x_n$. If $P \in C(\overline{\mathbb{Q}})$ is not a zero or pole of any function x_i, and the numbers $x_i(P)$ are multiplicatively dependent, there is $x \in \mathcal{X}$, x not identically 1, such that $x(P) = 1$. Now Proposition B′ yields

$$0 = h\big(x(P)\big) \ge \deg(x)h(P) - c \cdot \deg(x)\big(1 + \sqrt{h(P)}\big)$$

with c independent of x and P. Since by hypothesis, the function x cannot be a constant, we have $\deg(x) \geq 1$; therefore, $h(P) \leq c \cdot \left(1 + \sqrt{h(P)}\right)$. This proves Theorem 1′ and equivalently Theorem 1. ■

§3 An alternative argument

In this section, we develop an alternative approach to Theorem 1, which we also follow for the proof of Theorem 2.

Let Γ be a finitely generated subgroup of $\overline{\mathbb{Q}}^*$. We need a result giving generators of Γ, which are almost independent with respect to the Weil height. More precisely, we have the following lemma.

Lemma 2. Let Γ be a finitely generated subgroup of $\overline{\mathbb{Q}}^*$ of rank r. Then there are elements $g_1, \dots, g_r \in \Gamma$ generating a subgroup isomorphic to $\Gamma/\operatorname{tors}$ and such that

$$h\left(g_1^{a_1} \cdots g_r^{a_r}\right) \geq c(r)\left(|a_1|h(g_1) + \cdots + |a_r|h(g_r)\right)$$

for every $\mathbf{a} \in \mathbb{Z}^r$. Here $c(r)$ is a positive constant depending only on r, which may be taken as $c(r) = r^{-1}4^{-r}$. □

Proof. This is an immediate consequence of Theorem 1.1 of Schlickewei [Sc]. ■

Alternative proof of Theorem 1

For $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{Z}^n - \{0\}$, the rational function $x = x_1^{b_1} \cdots x_n^{b_n}$ is a nonconstant function on C; otherwise C would be contained in a proper coset $x_1^{b_1} \cdots x_n^{b_n} = a$.

The idea of the proof is based on the comparison of the height with respect to the function x with the height with respect to the coordinate functions x_j.

Let $P \in C(\overline{\mathbb{Q}})$ be such that $(x_1(P), \dots, x_n(P)) \in H$, where H is a proper algebraic subgroup of $\mathbb{G}_m^n$. Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be the group generated by the $x_i(P)$, and let r be its rank. Then $r < n$ because $P \in H(\overline{\mathbb{Q}})$ with $\dim(H) < n$; therefore, the $x_i(P)$ are multiplicatively dependent.

Let $g_1, \dots, g_r$ be generators of $\Gamma/\operatorname{tors}$ as in Lemma 2. We have

$$x_i(P) = \zeta_i g_1^{a_{i1}} \cdots g_r^{a_{ir}}$$

and

$$x(P) = \zeta g_1^{L_1(\mathbf{b})} \cdots g_r^{L_r(\mathbf{b})},$$

where ζ_i, ζ are roots of unity and where we have abbreviated

$$L_j(\mathbf{b}) = \sum_{i=1}^{n} a_{ij} b_i.$$

We want to find a nonzero integral vector $\mathbf{b}$ such that the linear forms $L_j(\mathbf{b})$ are all small in absolute value. By a familiar argument (for a geometry of numbers approach, see [V, Th. 2, p. 544]), given a positive integer T, we may find integers b_i, not all zero, such that

$$|b_i| \le T, \qquad |L_j(\mathbf{b})| \le nAh(g_j)^{-1} T^{-(n-r)/r}$$

for $i = 1, \dots, n$, $j = 1, \dots, r$, and where we have abbreviated

$$A = \max_{ij} |a_{ij}| h(g_j).$$

In fact, for $0 \le b_i' \le T$, we have $A^{-1} h(g_j) L_j(\mathbf{b}') \in [-(n - m_j)T, m_j T]$, where m_j is the number of positive coefficients in the linear form L_j. By the pigeon-hole principle, if $(1 + T)^n > (1 + 1/\varepsilon)^r$, we obtain a nonzero integral solution of $|A^{-1} h(g_j) L_j(\mathbf{b})| < \varepsilon n T$, $j = 1, \dots, r$ with $|b_i| \le T$, and we can take $\varepsilon = T^{-n/r}$.

It follows that

$$\begin{aligned} h\big(x(P)\big) &= h\big(g_1^{L_1(\mathbf{b})} \cdots g_r^{L_r(\mathbf{b})}\big) \\ &\le |L_1(\mathbf{b})| h(g_1) + \cdots + |L_r(\mathbf{b})| h(g_r) \\ &\le rnAT^{-(n-r)/r}. \end{aligned} \tag{3.1}$$

Let (i_0, j_0) be any (i, j) for which $|a_{ij}| h(g_j)$ reaches its maximum, and define the rational function y on C by

$$y = x_{i_0}.$$

Note that $\deg(y) \ge 1$ because otherwise x_{i_0} would be a constant on C, and C would be contained in translate of a proper algebraic subgroup of $\mathbb{G}_m^n$. By Lemma 2, we also have

$$h\big(y(P)\big) = h\big(g_1^{a_{i_0 1}} \cdots g_r^{a_{i_0 r}}\big) \ge c_1 A, \tag{3.2}$$

where $c_1 > 0$ depends only on r. Thus by (3.1) and (3.2), we get

$$\frac{h\big(x(P)\big)}{h\big(y(P)\big)} \le c_2 T^{-(n-r)/r}, \tag{3.3}$$

where c_2 depends only on n. We choose $T = \left[\left(2c_2 \deg(y)\right)^{r/(n-r)}\right] + 1$. Then, since the integers b_i are bounded by T, the function x belongs to a finite set independent of the point P. Hence, by Proposition B, there exists a positive number B, also independent of P, such that if $h(y(P)) \geq B$, we have

$$\frac{h\big(x(P)\big)}{h\big(y(P)\big)} \geq \frac{2}{3}\frac{\deg(x)}{\deg(y)}. \tag{3.4}$$

Now (3.3) and (3.4) yield

$$T \leq \left(\frac{3}{2}c_2 \deg(y)\right)^{r/(n-r)},$$

contradicting our choice of T. Thus we conclude that $h\big(y(P)\big) \leq B$. If we combine this inequality with (3.2), we get

$$c_1 A \leq h\big(y(P)\big) \leq B. \tag{3.5}$$

On the other hand, we have

$$h\big(\big(x_1(P), \ldots, x_n(P)\big)\big) = \sum_{i=1}^{n} h\big(x_i(P)\big) = \sum_{i=1}^{n} h\big(g_1^{a_{i1}} \cdots g_r^{a_{ir}}\big) \leq nrA. \tag{3.6}$$

By (3.5) and (3.6), we get[2]

$$h(P) \ll h\big(\big(x_1(P), \ldots, x_n(P)\big)\big) \leq \frac{nrB}{c_1},$$

concluding the proof. ∎

§4 Proof of Theorem 2

Let H be an algebraic subgroup of $\mathbb{G}_m^n$, of dimension $\leq n-2$. Fix $P \in C \cap H$; as noted before in the third remark after the statement of Theorem 1, $P \in C(\overline{\mathbb{Q}})$. Let Γ be the multiplicative group generated by the coordinates of P. Then the rank r of Γ does not exceed $n-2$, because $P \in H$ and $\dim(H) \leq n-2$. Theorem 2 is trivial if $r = 0$, because C contains only a finite number of torsion points; so in the rest of this paper, we assume that $n \geq 3$ and $r \geq 1$.

[2]We use Vinogradov's symbols $\gg$ and $\ll$ to denote inequalities up to an unspecified constant factor.

By applying Lemma 2 to Γ, we obtain good generators $g_1, \dots, g_r \in \Gamma$ of a subgroup isomorphic to $\Gamma/\operatorname{tors}$. In particular, $g_i \in \mathbb{Q}(P)$ and we may write

$$x_i(P) = \zeta_i g_1^{a_{i1}} \cdots g_r^{a_{ir}}, \quad i = 1, 2, \dots, n \tag{4.1}$$

for certain roots of unity ζ_i.

By Lemma 2 and Theorem 1, we have

$$|a_{ij}| h(g_j) \ll h\big(x_i(P)\big) \le h(P) \ll 1,$$

where the implied constants depend only on n and C. Therefore, setting

$$\boldsymbol{v}_j = \big(a_{1j}, \dots, a_{nj}\big)$$

and choosing i such that $|a_{ij}| = \max |\boldsymbol{v}_j|$, we see that

$$h(g_j) \ll |\boldsymbol{v}_j|^{-1}, \tag{4.2}$$

where $|\boldsymbol{v}_j|$ is the euclidean length.

Let us write $\zeta_i = \zeta^{l_i}$, where ζ is a primitive N-th root of unity. We assume N as small as possible here. Note that by (4.1), we have $\zeta \in \mathbb{Q}(P)$.

We apply Siegel's lemma as in [BV] to the $n+1$ linear forms $\sum_{i=1}^n a_{ij} b_i$, $j = 1, \dots, n$, and $\sum_{i=1}^n l_i b_i - N b_{n+1}$, in the $n+1$ variables b_i. The height of the relevant matrix is N times the height of the matrix $[a_{ij}]$, which in turn is estimated by the product of the euclidean length of its rows. Then we get a nonzero vector $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{Z}^n$ such that

$$\begin{aligned} &\sum_{i=1}^n a_{ij} b_i = 0, \quad j = 1, \dots, r, \\ &\sum_{i=1}^n l_i b_i \equiv 0 \pmod N, \end{aligned} \tag{4.3}$$

and

$$\max |b_i| \le \left(N \prod_{j=1}^r |\boldsymbol{v}_j| \right)^{1/(n-r)} = \big(N\Pi\big)^{1/(n-r)},$$

where we have abbreviated $\Pi = \prod_{j=1}^r |\boldsymbol{v}_j|$.

We have by (4.1) and (4.3) the equation

$$x_1(P)^{b_1} \cdots x_n(P)^{b_n} = 1.$$

The equation $x_1^{b_1} \cdots x_n^{b_n} = 1$ defines an algebraic subgroup H_1 of $\mathbb{G}_m^n$ of dimension $n-1$ and degree[3] bounded by $n \max|b_i|$. By assumption H_1 does not contain C, whence by Bézout's theorem, $H_1 \cap C$ contains at most $n \cdot \deg(C) \max|b_i|$ distinct points. Since it contains the point P, it also contains its conjugates over a field of definition for C, whence

$$\big[\mathbb{Q}(P) : \mathbb{Q}\big] \ll \max|b_i| \ll \big(N\Pi\big)^{1/(n-r)}. \tag{4.4}$$

Now we need a recent result of Amoroso and David that generalizes a well-known estimate by Dobrowolski [Do]. We state it in a slightly weaker but simpler form, sufficient for our purposes.

Lemma 3 (Amoroso and David). Let $\alpha_1, \ldots, \alpha_r$ be multiplicatively independent algebraic numbers generating a number field of degree $\le d$, and let $\varepsilon > 0$. Then

$$h(\alpha_1) \cdots h(\alpha_r) \gg d^{-1-\varepsilon},$$

where the implied constant depends only on ε and r. □

Proof. The proof is [AD, Théorème 1.6, p. 148], after replacing a power of $\log d$ by d^{ε}. ■

We apply this lemma with $\alpha_j = g_j$, $j = 1, \ldots, r$. We have already observed that $g_j \in \mathbb{Q}(P)$ for every j; thus we can take $d = [\mathbb{Q}(P) : \mathbb{Q}]$. After recalling (4.2), we obtain

$$\big(\big[\mathbb{Q}(P) : \mathbb{Q}\big]\big)^{-1-\varepsilon} \ll h(g_1) \cdots h(g_r) \ll \Pi^{-1}.$$

We combine this inequality with (4.4) and obtain

$$\Pi^{n-r-1-\varepsilon} \ll N^{1+\varepsilon} \tag{4.5}$$

as well as

$$\big[\mathbb{Q}(P) : \mathbb{Q}\big] \ll N^{1/(n-r-1-\varepsilon)},$$

provided $0 < \varepsilon < 1$.

[3]By degree of an irreducible affine variety $V \subset \mathbb{A}^n$, we mean the degree of the projective variety which is the closure of V in $\mathbb{P}^n$. If V is not irreducible, by degree we mean the sum of the degrees of its irreducible components of maximum dimension.

On the other hand, since $\zeta \in \mathbb{Q}(P)$, we have $\phi(N) \leq [\mathbb{Q}(P) : \mathbb{Q}]$, where $\phi(N)$ is Euler's function, and it is well known that $\phi(N) \gg N^{1-\varepsilon}$. We conclude that

$$N^{1-\varepsilon} \ll [\mathbb{Q}(P) : \mathbb{Q}] \ll N^{1/(n-r-1-\varepsilon)}. \tag{4.6}$$

The proof of Theorem 2 when $r \leq n-3$ is now almost immediate. If $r \leq n-3$, we have $n-r-1-\varepsilon \geq 2-\varepsilon$; therefore, for ε small enough, (4.6) implies that N and $[\mathbb{Q}(P) : \mathbb{Q}]$ are uniformly bounded independently of P and H. Thus the coordinates $x_i(P)$ have bounded degree over $\mathbb{Q}$ and, by Theorem 1, bounded height. By Northcott's theorem, they belong to a finite set, completing the proof.

Therefore, from now on, we assume that $r = n-2$. For the reader's convenience, to illustrate the strategy in this case, we sketch first the argument in the special case $n = 3$ (so $r = 1$), writing for brevity g in place of g_1.

To begin with, assume that some conjugate g' of g is multiplicatively independent with g. Then Lemma 2 applied to g, g' gives $h(g)h(g') \gg d^{-1-\varepsilon}$ with $d = [\mathbb{Q}(g, g') : \mathbb{Q}]$. Since $h(g) = h(g')$, we deduce that

$$h(g) \gg d^{-(1+\varepsilon)/2}. \tag{$*$}$$

On the other hand, d is now larger than $[\mathbb{Q}(P) : \mathbb{Q}]$, but not by much. This is because the fields $\mathbb{Q}(P) = \mathbb{Q}(g, \zeta)$ and its conjugate $\mathbb{Q}(g', \zeta)$ both contain $\mathbb{Q}(\zeta)$. Therefore, if $F = \mathbb{Q}(g, g', \zeta)$ is the composite field, we have

$$[F : \mathbb{Q}] \leq \frac{[\mathbb{Q}(g, \zeta) : \mathbb{Q}]^2}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} \ll N^{1+4\varepsilon}$$

if $\varepsilon \leq 1/5$, which we may suppose. Now combining the lower bound for $h(g)$ with (4.2) leads to $\Pi \ll N^{(1+\varepsilon)(1+4\varepsilon)/2}$; and then from (4.4) and (4.6) we see (taking for example $\varepsilon \leq 1/10$) that N is bounded, and we conclude as before.

What if the above multiplicative independence assumption is not satisfied? Then one can show that

(a) some power g^l ($l \geq 1$) lies in a quadratic extension L of $\mathbb{Q}$;

(b) if u is the norm of g from $L(g, \zeta)$ to $L(\zeta)$, then some ωu^k lies in L for some root of unity ω and some positive integer $k \leq 6$.

Now (a) implies that u is not a root of unity, and then (b) implies $h(u) \gg 1$; therefore,

$$h(g) \gg \frac{1}{[L(g, \zeta) : L(\zeta)]} \gg \frac{[\mathbb{Q}(\zeta) : \mathbb{Q}]}{[L(P) : \mathbb{Q}]} \gg N^{-3\varepsilon},$$

which is even better than the previous bound $(*)$ and suffices to complete the argument.

In the general case, the above argument is formalized as follows.

Lemma 4. Suppose that $r = n - 2$ and $h(g_1) \le h(g_j)$ for every j and that there is a conjugate g' of g_1 which is multiplicatively independent from $g_1, \dots, g_r$. Then N and $[\mathbb{Q}(P) : \mathbb{Q}]$ are uniformly bounded. □

Proof. Put $F = \mathbb{Q}(P, g')$. Then, since F contains the normal field $\mathbb{Q}(\zeta)$, we have

$$[F : \mathbb{Q}] \le \frac{\left[\mathbb{Q}(P) : \mathbb{Q}\right]^2}{\left[\mathbb{Q}(\zeta) : \mathbb{Q}\right]} \le N^{1+4\varepsilon}. \tag{4.7}$$

Now we apply Lemma 3 to $g', g_1, \dots, g_r$, getting

$$h(g')h(g_1)\cdots h(g_r) \gg N^{-(1+\varepsilon)(1+4\varepsilon)},$$

whence

$$h(g_1)\cdots h(g_r) \gg N^{-(1+\varepsilon)(1+4\varepsilon)r/(r+1)}$$

because $h(g') = h(g_1)$ has smallest height among the g_j. Combining this inequality with (4.2), we infer

$$\Pi \ll N^{(r/(r+1))+5\varepsilon}$$

at least if ε is sufficiently small. In view of (4.4), we finally obtain

$$N^{1-\varepsilon} \ll \left[\mathbb{Q}(P) : \mathbb{Q}\right] \ll N^{((2r+1)/(2r+2))+3\varepsilon}.$$

The lemma follows by taking ε sufficiently small. ■

Lemma 5. Given r, there is a positive integer $d(r)$, depending only on r, with the following property. Let $\alpha_1, \dots, \alpha_r$ be nonzero multiplicatively independent algebraic numbers, and let β be a nonzero algebraic number such that $\sigma(\beta), \alpha_1, \dots, \alpha_r$ are multiplicatively dependent for every σ in the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then there is a positive integer h such that β^h has degree at most $d(r)$ over $\mathbb{Q}$. □

Proof. Let s be the rank of the multiplicative group generated by β and all its conjugates $\sigma(\beta)$ over $\mathbb{Q}$. From our assumption about β, it follows that $s \le r$. Let $\boldsymbol{\beta} = (\beta_1, \dots, \beta_s)$ be a set of s multiplicatively independent conjugates of β. Then, for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exist

rational numbers $m_j(\sigma, i)$ and roots of unity $\rho_{\sigma,i}$ such that

$$\sigma(\beta_i) = \rho_{\sigma,i} \prod_{j=1}^{s} \beta_j^{m_j(\sigma,i)}, \quad i = 1, \dots, s.$$

We may abbreviate these equations symbolically as

$$\sigma(\boldsymbol{\beta}) = \boldsymbol{\rho}_\sigma \boldsymbol{\beta}^{M_\sigma},$$

where $\boldsymbol{\rho}_\sigma$ is a torsion point and M_σ is an $s \times s$ matrix with rational entries. From this equation and the fact that the β_i are multiplicatively independent, we derive the rule $M_\sigma M_\tau = M_{\sigma\tau}$; i.e., M is a homomorphism μ from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to the general linear group $\mathrm{GL}_s(\mathbb{Q})$. If σ fixes all the β_i's, then $M_\sigma = 1$, because the β_i's are multiplicatively independent. Therefore, the kernel of μ has finite index and μ has finite image.

Now, by [Bu, Note G, pp. 479–484], the order of any finite group of $s \times s$ matrices with entries in $\mathbb{Q}$ is bounded solely and explicitly in terms of s. Therefore, the index of the kernel of μ is bounded in terms of s only. Plainly, there exists a positive integer h such that $\rho_{\sigma,i}^h = 1$ for every σ and i; hence the kernel of μ fixes $\boldsymbol{\beta}^h$. If L denotes the fixed field of the kernel of μ, then the degree of L is bounded only in terms of s, whence only in terms of r, and moreover $\boldsymbol{\beta}^h \in L$, concluding the proof[4]. ■

The next lemma helps to control the size of the integer h in Lemma 5.

Lemma 6. Let L be a number field. Suppose that $u \neq 0$ lies in an abelian extension of L and that, for a positive integer h, we have $u^h \in L$. Then there exist a positive divisor k of h and a root of unity ω such that L contains the k-th roots of unity and $\omega u^k \in L$. In particular, $\phi(k) \leq [L : \mathbb{Q}]$. □

Proof. Let $\boldsymbol{\mu}$ denote the group of roots of unity, and define the subgroup S of $\mathbb{Z}$ by

$$S = \{m \in \mathbb{Z} : u^m \in \boldsymbol{\mu} L^*\}.$$

Then S contains the positive integer h and has a positive generator k that divides h. It suffices to prove that L contains the k-th roots of unity. Replacing u with ηu for a suitable root of unity η, we may assume that $u^k \in L$. Note that this substitution preserves S and the fact that $L(u)/L$ is abelian.

Let G be the abelian group $\mathrm{Gal}\big(L(u)/L\big)$, and let ζ denote a primitive k-th root of unity. Observe that, since $\sigma(u^k) = u^k$ for $\sigma \in G$, we have $\zeta \in L(u)$ and both $\sigma(u)/u$ and

[4]If $r = 1$ in Lemma 5, then $s = 1$ and so $[L : \mathbb{Q}] \leq 2$ as in (a) above.

$\sigma(\zeta)$ are powers of ζ; hence we may define functions $\chi : G \to (\mathbb{Z}/(k))^*$, $\psi : G \to \mathbb{Z}/(k)$ by

$$\sigma(\zeta) = \zeta^{\chi(\sigma)}, \qquad \sigma(u) = \zeta^{\psi(\sigma)} u.$$

Using the fact that G is abelian and equating the two expressions for $\tau(\sigma(u)) = \sigma(\tau(u))$, for $\sigma, \tau \in G$, we easily obtain

$$\psi(\sigma)\big(\chi(\tau) - 1\big) = \psi(\tau)\big(\chi(\sigma) - 1\big).$$

Fix for the moment $\tau \in G$, and let a, b be positive integers congruent, respectively, to $\psi(\tau)$, $\chi(\tau) - 1$, modulo k. Then we have, for any $\sigma \in G$,

$$\sigma\big(u^b\big) = \sigma(u)^b = \zeta^{\psi(\sigma)b} u^b = \zeta^{a(\chi(\sigma)-1)} u^b = \left(\frac{\sigma(\zeta)}{\zeta}\right)^a u^b;$$

thus u^b/ζ^a is fixed by σ and so lies in L^*. It follows that $b \in S$, and so b is a multiple of the generator k of S, showing that $\chi(\tau) = 1$ in $\mathbb{Z}/(k)$. This means precisely that τ fixes the k-th roots of unity. Because $\tau \in G$ was arbitrary, the k-th roots of unity must lie in L. This completes the proof[5] of Lemma 6. ■

Conclusion of the proof of Theorem 2

We have already verified the result if $r \le n-3$. Hence, by Lemma 4, we need only consider the case in which $r = n-2$, $h(g_1) \le h(g_j)$ for $j = 1, \dots, r$ and $g', g_1, \dots, g_r$ are multiplicatively dependent for every conjugate g' of g_1. By Lemma 5, there exist integers h, $d(r)$ such that g_1^h has degree $\le d(r)$ over $\mathbb{Q}$. Let $L = \mathbb{Q}(g_1^h)$, so that $[L : \mathbb{Q}] \le d(r)$. Define u to be the norm of g_1 from $L(P)$ to $L(\zeta)$, where, as in the beginning of this section, $\zeta \in \mathbb{Q}(P)$ is a primitive N-th root of unity with $\zeta_i = \zeta^{l_i}$ in (4.1). Since every conjugate of g_1 over L is of the form ηg_1 for some h-th root of unity η, we have

$$u = \eta' g_1^a, \tag{4.8}$$

where again η' is an h-th root of unity and $a = [L(P) : L(\zeta)]$. Now by (4.6), we have

$$\big[L(P) : L(\zeta)\big] \le \big[\mathbb{Q}(P) : \mathbb{Q}(\zeta)\big] \ll N^{1/(1-\varepsilon)-(1-\varepsilon)} \le N^{3\varepsilon}$$

if $\varepsilon \le 1/2$, which we may suppose. Observe that $u^h \in L$ and that u lies in an abelian extension $L(\zeta)$ of L. Therefore, we may apply Lemma 6 and deduce that there exist an

[5] If $[L : \mathbb{Q}] \le 2$ as in (a) above, then $k \le 6$ as in (b) above.

integer k and a root of unity ω such that $\omega u^k \in L$ and $\phi(k) \le d(r)$. In particular, k is bounded only in terms of n and, by Northcott's theorem, we have $h(\omega u^k) \ge c > 0$, where c depends only on n, because $\omega u^k \in L$, $[L : \mathbb{Q}] \le d(r)$, and because $u = \eta' g_1^a$ cannot be a root of unity. In particular,

$$h(g_1) = \frac{h(\omega u^k)}{(ka)} \ge \frac{c}{\left(k \cdot \left[L(P) : L(\zeta)\right]\right)} \gg N^{-3\varepsilon}$$

and

$$h(g_1) \cdots h(g_r) \gg N^{-3r\varepsilon}.$$

For small ε, this suffices for concluding the proof as in the case $r \le n - 3$.

Acknowledgments

E. Bombieri thanks the Istituto Universitario di Architettura, Venezia. U. Zannier thanks the Mathematics Institute of the University of Basel and the School of Mathematics of the Institute for Advanced Study, Princeton, for the hospitality and support received during the preparation of this paper.

References

[AD] F. Amoroso and S. David, *Le probléme de Lehmer en dimension supérieure*, J. reine angew. Math. **513** (1999), 145–179.

[B] E. Bombieri, *On Weil's "théorème de décomposition,"* Amer. J. Math. **105** (1983), 295–308. (Corrections in P. Dèbes, *Quelques remarques sur un article de Bombieri concernant le théorème de décomposition de Weil*, Amer. J. Math. **107** (1985), 39–44.

[BV1] E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11–32.

[BV2] ———, *Addendum to: "On Siegel's lemma,"* Invent. Math. **75** (1984), 377.

[BZ] E. Bombieri and U. Zannier, *Algebraic points on subvarieties of* $\mathbb{G}_m^n$, Internat. Math. Res. Notices (IMRN) **1995**, 333–347.

[Bu] W. Burnside, *Theory of Groups of Finite Order*, 2d ed., Dover Publ., New York, 1955.

[CZ] P. B. Cohen and U. Zannier, *Multiplicative independence and bounded height*, *an example*, preprint, 1998.

[D] V. A. Demjanenko, *Rational points of a class of algebraic curves*, Amer. Math. Soc. Transl. (2) **66** (1968), 246–272.

[Do] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.

[L] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[M] Yu. Manin, *The* p*-torsion of elliptic curves is uniformly bounded*, Izv. Akad. Nauk SSSR **33** (1969), 433–438.

[Ma] D. Masser, *Specializations of finitely generated subgroups of abelian varieties*, Trans. Amer. Math. Soc. **311** (1989), 413–424.

[N] A. Néron, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. (2) **82** (1965), 249–331.

[O] T. Oda, *Convex Bodies and Algebraic Geometry*, Ergeb. Math. Grenzgeb. **15**, Springer-Verlag, Berlin, 1988.

[R] M. Raynaud, "Sous-variétés d'une variété abélienne et points de torsion" in *Arithmetic and Geometry*, *Vol. I*, dedicated to I. R. Shafarevitch, ed. M. Artin and J. Tate, Progr. Math. **35**, Birkhäuser, Boston, 1983.

[S] A. Schinzel, *Reducibility of lacunary polynomials X*, Acta Arith. **53** (1989), 47–97.

[Sc] H. P. Schlickewei, *Lower bounds for heights on finitely generated groups*, Monatsh. Math. **123** (1997), 171–178.

[Si] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. **1** (1929), 41–69.

[Sil] J. Silverman, *Heights and the specialization map for families of abelian varieties*, J. reine angew. Math. **342** (1983), 197–211.

[V] J. D. Vaaler, *A geometric inequality with applications to linear forms*, Pacific J. Math. **83** (1979), 543–553.

Bombieri: School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540, USA; eb@math.ias.edu

Masser: Mathematisches Institut Universität Basel, Rheinsprung 21, CH-4501 Basel, Switzerland; masser@math.unibas.ch

Zannier: Istituto Universitario di Architettura-DCA, S. Croce 191, 30135 Venezia, Italy; zannier@iuav.unive.it