Atti Accademia Nazionale Lincei Classe Scienze Fisiche Matematiche Naturali

Rendiconti Lincei
Matematica e Applicazioni

Enrico Bombieri, Umberto Zannier

A Note on heights in certain infinite extensions of $\mathbb{Q}$

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Serie 9, Vol. **12** (2001), n.1, p. 5–14.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLIN_2001_9_12_1_5_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Accademia Nazionale dei Lincei, 2001.

Rend. Mat. Acc. Lincei
s. 9, v. 12:5-14 (2001)

Teoria dei numeri. — *A* Note *on heights in certain infinite extensions of* $\mathbb{Q}$. Nota di
Enrico Bombieri e Umberto Zannier, presentata (*) dal Socio E. Bombieri.

Abstract. — We study the behaviour of the absolute Weil height of algebraic numbers in certain infinite extensions of $\mathbb{Q}$. In particular, we obtain a Northcott type property for infinite abelian extensions of finite exponent and also a Bogomolov type property for certain fields which are a p-adic analog of totally real fields. Moreover, we obtain a non-archimedean analog of a uniform distribution theorem of Bilu in the archimedean case.

Key words: Algebraic number theory; Heights; Uniform distribution.

Riassunto. — *Una* Nota *sulle altezze in estensioni infinite di* $\mathbb{Q}$. In questa *Nota* si studia il comportamento dell'altezza di numeri algebrici in certe estensioni infinite dei numeri razionali. In particolare, si ottengono l'estensione della proprietà di Northcott ad estensioni abeliane infinite ma di esponente finito, e l'estensione della proprietà di Bogomolov a corpi che sono l'analogo p-adico del corpo dei numeri algebrici totalmente reali. In questo modo, si ricava anche un analogo non-archimedeo del teorema di distribuzione uniforme dei coniugati di Galois, ottenuto da Bilu nel caso archimedeo.

1. Introduction

We say that a set $\mathcal{A}$ of algebraic numbers has the *Northcott property* (N) if for every positive real number T the set

$$\mathcal{A}(T) = \{\alpha \in \mathcal{A} : h(\alpha) < T\}$$

is finite; here $h(\alpha)$ denotes the absolute logarithmic Weil height.

A well-known theorem of Northcott [7], which has many useful applications, states that the set of all algebraic numbers of degree at most d has property (N).

One may ask if property (N) holds for other interesting sets. For example, does it hold for the field $\mathbb{Q}^{(d)}$, the composite field of all number fields of degree at most d over $\mathbb{Q}$? Although this question remains open in general, we shall show that this is the case if $d = 2$. More generally, we show that property (N) holds for the maximal abelian subfield of $\mathbb{Q}^{(d)}$.

We also say that a set $\mathcal{A}$ of algebraic numbers has the *Bogomolov property* (B) if there exists a positive real number T_0 such that $\mathcal{A}(T_0)$ consists of all roots of unity in $\mathcal{A}$. There are several interesting examples of infinite degree fields with property (B), among them the infinite cyclotomic extension of $\mathbb{Q}$ generated by all roots of unity [1, 2] and the field of all totally real algebraic numbers [9-11]. We shall give an extension of this latter result and relate it to the uniform distribution of points of small height with respect to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, as in the work of Bilu [3]. We also give an

(*) Nella seduta del 15 dicembre 2000.

extension of Bilu's result to a p-adic setting and deduce from this some new cases of infinite fields with property (B).

2. The Northcott property

Let K be a number field and denote by $K^{(d)}$ the compositum of all extension fields F/K of degree at most d over K. Then $K^{(d)}$ is normal over K. We also denote by $K_{ab}^{(d)}$ the compositum of all abelian extensions L/K with $K \subseteq L \subseteq K^{(d)}$; then $K_{ab}^{(d)}$ is normal abelian over K.

If $d \geq 2$ the fields $K^{(d)}$ and $K_{ab}^{(d)}$ have infinite degree over K. However, the local degrees remain bounded, as the following result shows.

Proposition 1. *Let $v \in M_K$ be any place of K and let w be an extension of v to $K^{(d)}$ and let K_v, $K_w^{(d)}$ be the corresponding complete fields. Then the local degree $[K_w^{(d)} : K_v]$ is bounded in terms of d and $[K : \mathbb{Q}]$ alone, independently of v, w.*

Proof. Let us fix an algebraic closure Ω_v of K_v. It is well known that there are only finitely many extensions $K_v \subseteq L \subset \Omega_v$ of degree at most d, and their number is bounded only in terms of d and $[K_v : \mathbb{Q}_v]$ (see for instance [6: 4 (*ii*), p. 260]). Therefore, the degree of their compositum is bounded only in terms of d and $[K_v : \mathbb{Q}_v] \leq [K : \mathbb{Q}]$. Since $K_w^{(d)}$ may be embedded in such a compositum, the proposition follows.

Proposition 1 raises the question whether the Northcott property holds for any field $F \subset \overline{\mathbb{Q}}$ such that $[F_w : \mathbb{Q}_v]$ is uniformly bounded for $w \in M_F$. We do not know the answer to this question, but it is a simple exercise, using Tchebotarev's Density Theorem, to show that such an assertion is equivalent to the validity of (N) for $K^{(d)}$, $d \geq 2$. On the other hand, we can prove

Theorem 1. *Property (N) holds for the field $K_{ab}^{(d)}$, for any $d \geq 2$.*

Corollary 1. *The field $K^{(2)}$ has the Northcott property.*

Proof. Obvious, because $K^{(2)} = K_{ab}^{(2)}$.

Corollary 2. *For any $m \geq 2$ the field $\mathbb{Q}(\sqrt[m]{1}, \sqrt[m]{2}, \sqrt[m]{3}, \dots)$ has the Northcott property.*

Proof. Let $K = \mathbb{Q}(\sqrt[m]{1})$. Then each field $K(\sqrt[m]{a})$ is of degree at most m and abelian over K. Therefore, their compositum $F = \mathbb{Q}(\sqrt[m]{1}, \sqrt[m]{2}, \sqrt[m]{3}, \dots)$ is abelian over K and a subfield of $K_{ab}^{(m)}$. By Theorem 1, $K_{ab}^{(m)}$ has the Northcott property and the same holds for its subfield F.

Proof of Theorem 1. In what follows, we abbreviate $D = d!$. In proving Theorem 1, we may enlarge the number field K, hence may suppose that K contains the field $\mathbb{Q}(\sqrt[D]{1})$ generated by roots of unity of order D. Let us fix a positive real number T and let $\alpha \in K_{ab}^{(d)}$ satisfy $h(\alpha) \leq T$. Let $L = K(\alpha)$; L is automatically normal over K, as a subfield of an abelian field, and is a finite abelian extension of K of exponent dividing D. Let p be a prime, unramified in K and let v be a place of K above p. Let e be the ramification index of v in L. If $p > d$, p will be tamely ramified in L, because any prime dividing the order of $\mathrm{Gal}(L/K)$ does not exceed d. Since p is tamely ramified, any inertia group above v is cyclic, of order e dividing D.

Now let $\theta = p^{1/e}$ for some choice of the root, and consider the field $L(\theta)$. The ramification index of $K(\theta)/K$ at any place w above v is e. By Abhyankar's lemma [6, Corollary 4, p. 236], $L(\theta)/L$ is unramified at w. Therefore, the ramification indices above v in $L(\theta)$ are again e. Let $I \subset \mathrm{Gal}(L(\theta)/K)$ be the inertia group at w, a group of order e. Since $L(\theta)/K$ is abelian, all the inertia groups above v are equal to I. Define U as the fixed field of I. Then U is normal over K and v is unramified in U. Also, $[L(\theta) : U] = |I| = e$. Observe that $U \cap K(\theta) = K$, since v is unramified in U and totally ramified in $K(\theta)$. Hence $[U(\theta) : U] = e$, proving in particular that $U(\theta) = L(\theta)$. It follows that $\alpha \in U(\theta)$ and we may write

$$\alpha = \beta_0 + \beta_1\theta + \ldots + \beta_{e-1}\theta^{e-1}, \qquad \beta_i \in U.$$

The conjugates of θ over U are $\zeta^r\theta$, where ζ is a primitive e-th root of unity and $r = 0, 1, \ldots, e-1$. Therefore, the trace $\mathrm{Trace}_U^{U(\theta)}(\theta^j)$ vanishes if j is not a multiple of e and equals e if $j = 0$. Hence

$$\beta_j = \frac{1}{e}\mathrm{Trace}_U^{U(\theta)}(\alpha\theta^{-j}) = \frac{1}{ep^{j/e}}\sum_{r=0}^{e-1}\zeta^{-jr}\alpha_r$$

where α_r are certain conjugates of α; note that $h(\alpha_r) = h(\alpha) \le T$ for $0 \le r \le e-1$. By a standard inequality about the height of a sum we find

$$h(\beta_j p^{j/e}) \le \log e + \sum_r h(\alpha_r) + \log e \le 2\log D + DT. \tag{1}$$

As before, let w be any place of $U(\theta) = L(\theta)$ above v and use the same letter to denote the associated normalized order function. Since $\beta_j \in U$ we have that $w(\beta_j)$ is divisible by e. Suppose now $1 \le j \le e-1$. Then $w(p^{j/e}) = j$ is not divisible by e, whence $w(\beta_j p^{j/e}) \ne 0$. This shows that $|w(\beta_j p^{j/e})| \ge w(p^{1/e}) = 1$.

Let us abbreviate $\gamma = \beta_j p^{j/e}$ and suppose that $\gamma \ne 0$. We have by definition $|\gamma|_w = |\mathrm{Norm}(\gamma)|_p^{1/\delta}$, where the norm is from $U(\theta)_w$ to $\mathbb{Q}_p$ and $\delta := [U(\theta) : \mathbb{Q}]$. Also, letting δ_w be the local degree $\delta_w := [U(\theta)_w : \mathbb{Q}_p]$, we have that $|\mathrm{Norm}(\gamma)|_p^{1/\delta_w}$ extends the usual p-adic absolute value, and in particular takes values in the group generated by $p^{1/e}$. Since γ has nontrivial order at w, we see that $\mathrm{Norm}(\gamma)$ has nontrivial order at p, whence $\big|\log|\gamma|_w\big| \ge (\delta_w/e\delta)\log p$. Thus we have

$$2h(\gamma) = h(\gamma) + h(\gamma^{-1}) \ge \sum_{w|v}\big|\log|\gamma|_w\big| \ge \frac{1}{e\,[U(\theta) : \mathbb{Q}]}\left(\sum_{w|v}\delta_w\right)\log p.$$

Since $\sum\delta_w$ is the sum of the local degrees above v, we have $\sum\delta_w = [U(\theta) : K]$.

Obviously, $[U(\theta):\mathbb{Q}] \leq [U(\theta):K]\cdot[K:\mathbb{Q}]$. We conclude that if $\gamma \neq 0$ then

$$2h(\gamma) \geq \frac{1}{e\,[K:\mathbb{Q}]}\log p.$$

Comparing with (1) we derive that either $\beta_j = 0$ or

$$\log p \leq 2e\,[K:\mathbb{Q}](2\log D + DT).$$

Let S be the set of primes $p > \exp(2e\,[K:\mathbb{Q}](2\log D + DT))$ which are unramified in K. We have shown that if $p \in S$ we must have $\beta_j = 0$ for $1 \leq j \leq e-1$. This means that for every place v of K lying above a prime $p \in S$ the algebraic number α lies in U, which is an abelian extension of K of exponent dividing D and unramified at v. Hence $K(\alpha)$ is unramified above any $p \in S$. Writing $\mathrm{Gal}(K(\alpha)/K)$ as a direct product of cyclic groups of order dividing D, we see that $K(\alpha)$ is the composite of cyclic extensions of K of degree at most D, each unramified at any prime of S. On the other hand, the power to which a prime divides the discriminant of a number field of bounded degree is itself bounded (see [6, Note 11, p. 80]). Hence the discriminants of these cyclic extensions of K are bounded. We conclude by Hermite's theorem [6, Theorem 2.12, p. 69] that there are only finitely many such cyclic fields. Hence there are only finitely many distinct fields $K(\alpha)$ and, since α has bounded height, there are only finitely many possibilities for α itself.

3. The Bogomolov property

For simplicity, we shall consider here only normal extensions L of $\mathbb{Q}$. Given such an extension, we denote by $S(L)$ the set of rational primes p such that L may be embedded in some finite extension L_p of $\mathbb{Q}_p$. We may also assume that the closure of L in L_p is again L_p, in which case, since L is normal, the residual degree f_p and ramification index e_p of the extension $L_p/\mathbb{Q}_p$ do not depend on the given embedding. We have

Theorem 2. *If $S(L)$ is not empty then the field L has the Bogomolov property. More precisely, we have*

$$\liminf_{\alpha\in L} h(\alpha) \geq \frac{1}{2}\sum_{p\in S(L)} \frac{\log p}{e_p(p^{f_p}+1)}. \tag{2}$$

Remark. If the sum on the right-hand side of (2) diverges, then L has property (N). Thus the question arises whether there are infinite extensions L where this occurs. We have been unable to find such examples, and we consider it unlikely that this can occur for an infinite extension.

Example 1. Let us say that a non-zero algebraic number α is totally p-adic if the rational prime p splits completely in the field $\mathbb{Q}(\alpha)$. Then the field L of all totally p-adic algebraic numbers is normal and $p \in S(L)$. Hence L has the Bogomolov property. This may be considered as the p-adic analog of results of Schinzel and Smyth for totally real algebraic numbers alluded to in Section 1.

EXAMPLE 2. Let $p_1, \ldots, p_m$ be distinct rational primes and let L be the field of all totally p-adic algebraic numbers for $p = p_1, \ldots, p_m$. Then it is clear that $p_i \in S(L)$ for $i = 1, \ldots, m$. Moreover, we have

$$\liminf_{\alpha \in L} h(\alpha) \leq \sum_{i=1}^{m} \frac{\log p_i}{p_i - 1}. \tag{3}$$

This shows that the lower bound given by (2) is of the correct order of magnitude, in so far as the contribution of primes with $f_p = e_p = 1$ is concerned.

We give now the proof of (3). To this end, we give an infinite sequence of totally p-adic algebraic numbers for $p = p_1, \ldots, p_m$ and satisfying (3). The idea is to construct a sequence of polynomials with small integral coefficients and arbitrarily large degree r, which are irreducible over $\mathbb{Q}$ but with all roots in the p-adic field $\mathbb{Q}_p$ for $p = p_1, \ldots, p_m$. We start with the polynomial

$$F(x) := (x-1)(x-2)\cdots(x-r)$$

and proceed to deform it into a polynomial with all desired properties.

Let us fix: a prime q distinct from the primes p_i, positive integers a_i for $i = 1, \ldots, m$, a monic polynomial $H(x) \in \mathbb{Z}[x]$ of degree r, which is irreducible mod q. Now, using the Chinese Remainder Theorem, choose a polynomial $f(x) \in \mathbb{Z}[x]$ of degree r such that

(*i*) $f(x) \equiv H(x) \pmod{q}$,

(*ii*) $f(x) \equiv F(x) \pmod{p_i^{a_i}}$ *for* $i = 1, \ldots, m$,

(*iii*) *the coefficients of* $f(x)$ *are non-negative and do not exceed* $q \prod p_i^{a_i}$.

It is clear by (*i*) that $f(x)$ is irreducible over $\mathbb{Q}$. If the integers a_i are sufficiently large, Hensel's lemma shows that $f(x)$ has r roots close to $1, \ldots, r$ in each field $\mathbb{Q}_{p_i}$, which would suffice to complete our construction. However, in this special case it is to our advantage to use directly Newton's approximation scheme. In what follows, we drop the suffix i writing p, a for p_i and a_i and denote by $v(\ )$ the usual p-adic valuation in $\mathbb{Q}_p$.

LEMMA 1. *Let* $f(x) \in \mathbb{Q}[x]$, $x_0 \in \mathbb{Q}_p$ *and define* $t := v(f'(x_0))$. *Let* b *be such that*

$$v\left(\frac{f^{(k)}(x_0)}{k!}\right) \geq t - (k-1)b$$

for $k \geq 2$ *and*

$$v(f(x_0)) > t + b.$$

Then the sequence of Newton approximations

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

converges in $\mathbb{Q}_p$ *to a root* α *of* $f(x)$ *such that*

$$v(\alpha - x_0) > v(f(x_0)) - t.$$

PROOF. It clearly suffices to verify by induction on n that

$$\begin{aligned} &v(f(x_{n+1})) > v(f(x_n)) > t + b\,,\\ &v(f'(x_{n+1})) = t\,,\\ &v\left(\frac{f^{(k)}(x_{n+1})}{k!}\right) \geq t - (k-1)b\,, \quad \textit{for } k \geq 2. \end{aligned}$$

This follows easily from Taylor's formula

$$\frac{f^{(k)}(x_{n+1})}{k!} = \sum_{\nu=0}^{\infty} \binom{k+\nu}{k} \frac{f^{(k+\nu)}(x_n)}{(k+\nu)!}(x_{n+1} - x_n)^{\nu}$$

and

$$v(x_{n+1} - x_n) = v(-f(x_n)/f'(x_n)) = v(f(x_n)) - t.$$

We apply several times Lemma 1 to $f(x)$, choosing $p = p_i$, $a = a_i$ and $x_0 = j$, for $i = 1, \ldots, m$ and $j = 1, \ldots, r$. In order to verify the hypothesis of the lemma, we need to compute bounds for $v(f^{(k)}(j)/k!)$. We shall use the easy estimate $v(n!) \leq$ $\leq (n-1)/(p-1)$, valid for $n \geq 1$.

For $k = 0$, it is immediate that $v(f(j)) \geq a$, because of the congruence (*ii*) and $F(j) = 0$.

For $k = 1$, we note that $F'(j) = \pm (j-1)! \cdot (r-j)!$; therefore, assuming $r \geq 2$, we get $v(F'(j)) \leq v((j-1)!) + v((r-j)!) \leq \frac{r-2}{p-1}$. Thus we have $t := v(f'(j)) = v(F'(j))$ as soon as $a > (r-2)/(p-1)$, which we shall suppose; note that $t \leq (r-2)/(p-1)$.

Finally, for $k \geq 2$ we note that

$$F^{(k)}(j) = k!\, F'(j) \sum_{\substack{|J|=k-1\\ j \notin J}} \prod_{h \in J} \frac{1}{j-h}\,,$$

with J running over all $(k-1)$-subsets of $\{1, \ldots, r\}$ not containing j. This gives

$$v(F^{(k)}(j)/k!) \geq t - (k-1) \max_{1 \leq l < r} v(l). \tag{4}$$

Using $a > t$ and $v(l) \leq [\log r/\log p]$ we get from the congruence (*ii*) and (4) the lower bound

$$v\left(\frac{f^{(k)}(j)}{k!}\right) \geq t - (k-1)b$$

with

$$b = \left[\frac{\log r}{\log p}\right].$$

By the upper bound $t \le (r-2)/(p-1)$, if

$$a > \frac{r-2}{p-1} + \left[\frac{\log r}{\log p}\right] \ge t + b\,,$$

which we shall suppose, the hypothesis of Lemma 1 is satisfied and then $f(x)$ has a root α_j in $\mathbb{Q}_p$ with $v(\alpha_j - j) > v(f(j)) - t$.

On the other hand, we have verified that $v(f(j)) \ge a$, and also we assumed the stronger condition $a > t + b$. Therefore, we have $v(\alpha_j - j) > b$. Since $v(j - j') \le b$ if $1 \le j < j' \le r$, it follows that $f(x)$ has r roots in $\mathbb{Q}_{p_i}$, $i = 1, \ldots, m$.

This completes the construction of the polynomial $f(x)$ and the only remaining thing to do is to estimate the height of its roots. The polynomial $f(x)$ is irreducible over $\mathbb{Q}$, has degree r and positive coefficients bounded by $q\prod p_i^{a_i}$. By a well-known estimate, this yields

$$h(\alpha) \le \frac{1}{r}\sum_{i=1}^{m} a_i \log p_i + \frac{\log(q\sqrt{r})}{r}.$$

If we choose a_i as small as possible, namely $a_i \sim r/(p_i - 1)$, and let $r \to \infty$ we obtain (3).

Proof of Theorem 2. We shall prove a general lower bound for the height of an algebraic number, of which Theorem 2 will be an easy corollary. Let K be a Galois extension of $\mathbb{Q}$, let $\alpha \in K^*$ and denote by $\alpha_1, \alpha_2, \ldots, \alpha_m$ a full set of conjugates over $\mathbb{Q}$, satisfying a minimal equation over $\mathbb{Z}$:

$$a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0 = 0.$$

Fix a rational prime p and denote by v an extension to K, of residual degree f_p and ramification index e_p, of the usual valuation in $\mathbb{Q}_p$. By reordering the conjugates, we may assume

$$v(\alpha_1) \ge \ldots \ge v(\alpha_r) \ge 0 > v(\alpha_{r+1}) \ge \ldots \ge v(\alpha_m).$$

By Gauss's lemma [4, Chapter IV, Theorem 2.1] we have

$$v(a_m) = -\sum_{i=r+1}^{m} v(\alpha_i). \tag{5}$$

Let Δ be the discriminant

$$\Delta := a_m^{2m-2}\prod_{i<j}(\alpha_i - \alpha_j)^2.$$

In order to evaluate $v(\Delta)$ from below we consider first the contribution to the product coming from terms with $v(\alpha_j) < 0$. We have

$$v\Bigg(\prod_{j=r+1}^{m}\prod_{i=1}^{j-1}(\alpha_i - \alpha_j)\Bigg) \ge \sum_{j=r+1}^{m}(j-1)\,v(\alpha_j)\,,$$

yielding the lower bound

$$v(\Delta) \geq (2m-2)\, v(a_m) + 2 \sum_{i<j\leq r} v(\alpha_i - \alpha_j) + 2 \sum_{j=r+1}^{m} (j-1)\, v(\alpha_j).$$

We substitute (5) in the right-hand side of this inequality and obtain

$$v(\Delta) \geq 2 \sum_{i<j\leq r} v(\alpha_i - \alpha_j) - 2 \sum_{j=r+1}^{m} (m-j)\, v(\alpha_j). \tag{6}$$

Consider now the reductions of α_i, $i \leq r$, modulo the maximal ideal of the valuation ring of v. They are elements of the finite field $\mathbb{F}_q$ with $q = p^{f_p}$. For $x \in \mathbb{F}_q$, let N_x be the number of conjugates α_i with reduction x. Suppose $i < j \leq r$. If α_i and α_j have the same reduction, we have $v(\alpha_i - \alpha_j) > 0$, hence $v(\alpha_i - \alpha_j) \geq 1/e_p$, and otherwise we have $v(\alpha_i - \alpha_j) \geq 0$; note that the number of pairs (i, j) with $i < j$ and such that α_i and α_j have the same reduction x is $N_x(N_x - 1)/2$. If instead $j > r$, we have $v(\alpha_j) < 0$, hence $v(\alpha_j) \leq -1/e_p$.

In view of these remarks, we deduce from (6) that

$$v(\Delta) \geq \frac{1}{e_p} \sum_{x\in\mathbb{F}_q} N_x(N_x - 1) + \frac{1}{e_p}\,(m-r)(m-r-1). \tag{7}$$

A more elegant formulation of (7) is obtained by defining the reduction of an element with negative valuation to be ∞. With this convention, N_∞ is simply $N_\infty = m - r$ and $\sum_{x\in\mathbb{F}_q\cup\infty} N_x = m$. Therefore, introducing the normalized variance

$$V_p(\alpha; K) := \frac{1}{m^2} \sum_{x\in\mathbb{F}_q\cup\infty} \left(N_x - \frac{m}{q+1} \right)^2 \tag{8}$$

we rewrite (7) as

$$v(\Delta) \geq \frac{m^2}{e_p} \left(V_p(\alpha; K) + \frac{1}{q+1} \right) - \frac{m}{e_p}\,. \tag{9}$$

This estimate is useful only in the range $q < m$ but, since Δ is a non-zero rational integer, we have $v(\Delta) \geq 0$ in any case. Thus from (9) it follows that

$$\log|\Delta| \geq m^2 \sum_{q<m} \frac{1}{e_p} \left(V_p(\alpha; K) + \frac{1}{q+1} - \frac{1}{m} \right) \log p. \tag{10}$$

On the other hand, we have a classic inequality of Mahler [5, Theorem 1]

$$\log|\Delta| \leq m \log m + (2m-2)\, m\, h(\alpha). \tag{11}$$

Therefore, combining (10) and (11) we finally obtain

THEOREM 3. *Let K be a Galois extension of $\mathbb{Q}$ and for each rational prime p let f_p and e_p be the residual degree and ramification index of p in K. Let also $\mathfrak{p}$ a prime ideal of K dividing (p) and write $q := p^{f_p}$.*

Let $\alpha \in K^*$ *be of degree* m *and let* $V_p(\alpha; K)$ *be the normalized variance*

$$V_p(\alpha; K) := \frac{1}{m^2} \sum_{x \in \mathbb{F}_q \cup \infty} \left(N_x - \frac{m}{q+1} \right)^2,$$

where, for $x \in \mathbb{F}_q$, N_x *is the number of conjugates of* α *with reduction* x *modulo* $\mathfrak{p}$ *and* N_∞ *is the number of conjugates of* α *which are not integers in* $K_\mathfrak{p}$. *This variance does not depend on the choice of* $\mathfrak{p}|p$.

Then we have

$$h(\alpha) \geq -\frac{\log m}{2m-2} + \frac{m}{2m-2} \sum_{q<m} \frac{1}{e_p} \left(V_p(\alpha; K) + \frac{1}{q+1} - \frac{1}{m} \right) \log p.$$

The proof of Theorem 2 is now easy. For $\alpha \in L$ we apply Theorem 3 with K the Galois closure of α and note that the numbers f_p, e_p relative to the field K do not exceed the corresponding quantities for the field L. Since $V_p(\alpha; K) \geq 0$ in any case, the proof is completed by noting that, by Northcott's theorem, in any infinite sequence of distinct algebraic numbers of bounded height the degrees must go to ∞, hence we have $m \to \infty$ if we want to estimate $\liminf h(\alpha)$ in L.

REMARK. Theorem 3 implies an equidistribution theorem for elements of an infinite sequence $\{\alpha\}$ of algebraic numbers with height tending to 0. In particular, for any sequence $\{\alpha\}$ along which $h(\alpha) \to 0$, we have that if p is unramified in the Galois closure of α then $q := p^{f_p} \to \infty$ and

$$\frac{1}{\deg^2(\alpha)} \sum_{x \in \mathbb{F}_q \cup \infty} \left(N_x - \frac{\deg(\alpha)}{q+1} \right)^2 \log p \to 0. \tag{12}$$

This may be regarded as an analog of Bilu's equidistribution theorem [3]; see also [8] for related results in a p-adic and adelic setting.

ACKNOWLEDGEMENTS

This work has been supported by a grant of GNSAGA to E. Bombieri and by a grant to the Institute for Advanced Study by the James D. Wolfensohn Fund to U. Zannier.

REFERENCES

[1] F. AMOROSO - R. DVORNICICH, *A lower bound for the height in abelian extensions*. J. Number Th., 80, 2000, 260-272.
[2] F. AMOROSO - U. ZANNIER, *A relative Dobrowolski's lower bound over abelian extensions*. Preprint 1999; Annali Sc. Norm. Sup. Pisa, to appear.
[3] Y. BILU, *Limit distribution of small points on algebraic tori*. Duke Math. J., 89, 1997, 465-476.
[4] S. LANG, *Algebra*. 3rd ed., Addison-Wesley, 1994, xv + 912 pp.
[5] K. MAHLER, *An inequality for the discriminant of a polynomial*. Michigan Math. J., 11, 1964, 257-262.
[6] W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*. PWN - Polish Scientific Publishers & Springer-Verlag, Warszawa 1990, xiv + 746 pp.
[7] D.G. NORTHCOTT, *An inequality on the theory of arithmetic on algebraic varieties*. Proc. Cambridge Philos. Soc., 45, 1949, 502-509.

[8] R. RUMELY, *On Bilu's equidistribution theorem*. In: *Spectral problems in geometry and arithmetic* (Iowa City IA 1997). Contemp. Math., 237, AMS, Providence RI 1999, 159-166.
[9] A. SCHINZEL, *On the product of the conjugates outside the unit circle of an algebraic number*. Acta Arith., 24, 1973, 385-399. Addendum *ibidem*, 26, 1973, 329-361.
[10] C.J. SMYTH, *On the measure of totally real algebraic numbers*. (I). J. Austral. Math. Soc., Ser. A, 30, 1980-81, 137-149.
[11] C.J. SMYTH, *On the measure of totally real algebraic numbers*. (II). Math. Comp., 37, 1981, 205-208.

Pervenuta il 27 settembre 2000,
in forma definitiva il 9 dicembre 2000.

E. Bombieri:
Institute for Advanced Study
School of Mathematics
PRINCETON, NJ 08540 (U.S.A.)
eb@ias.edu

U. Zannier:
Istituto Universitario di Architettura
Santa Croce, 191 - 30135 VENEZIA
zannier@iuav.unive.it