ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

FRANCESCO AMOROSO
UMBERTO ZANNIER

A relative Dobrowolski lower bound over abelian extensions

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 29, nº 3 (2000), p. 711-727
<http://www.numdam.org/item?id=ASNSP_2000_4_29_3_711_0>

© Scuola Normale Superiore, Pisa, 2000, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (http://www.sns.it/it/edizioni/riviste/annaliscienze/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)
Vol. XXIX (2000), pp. 711-727

A Relative Dobrowolski Lower Bound over Abelian Extensions

FRANCESCO AMOROSO - UMBERTO ZANNIER

Abstract. Let α be a non-zero algebraic number, not a root of unity. A well-known theorem by E. Dobrowolski provides a lower bound for the Weil height $h(\alpha)$ which, in simplified form, reads $h(\alpha) \gg D^{-1-\varepsilon}$, where $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. On the other hand, F. Amoroso and R. Dvornicich have recently found that if α lies in an abelian extension of the rationals, then $h(\alpha)$ is bounded below by a positive number independent of D. In the present paper we combine these results by showing that, in the above inequality, D may be taken to be the degree of α over any abelian extension of a fixed number field. As an application, we also derive a new lower bound for the Mahler measure of a polynomial in several variables, with integral coefficients.

Mathematics Subject Classification (2000): 11G50 (primary), 11Jxx (secondary).

1. - Introduction

Let α be a non zero algebraic number which is not a root of unity. Then, by a theorem of Kronecker, the absolute logarithmic Weil height $h(\alpha)$ is > 0. More precisely, let $\mathbb{K}$ be any number field containing α. By using Northcott's theorem (see [No]), it is easy to see that $h(\alpha) \geq C(\mathbb{K})$, where $C(\mathbb{K}) > 0$ is a constant depending only on $\mathbb{K}$. In other words, 0 is not an accumulation point for the height in $\mathbb{K}$.

In a remarkable paper, Lehmer [Le] asked whether there exists a positive absolute constant C_0 such that

$$h(\alpha) \geq \frac{C_0}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

This problem is still open, the best unconditional lower bound in this direction being a theorem of Dobrowolski [Do], who proved:

$$h(\alpha) \geq \frac{C_1}{D}\left(\frac{\log(3D)}{\log\log(3D)}\right)^{-3}, \qquad D = [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

Pervenuto alla Redazione il 11 novembre 1999 e in forma definitiva il 2 maggio 2000.

for some absolute constant $C_1 > 0$. However, in some special cases not only the inequality conjectured by Lehmer is true, but it can also be sharpened. Assume for instance that $\mathbb{Q}(\alpha)$ is an abelian extension of the rational field. Then the first author and R. Dvornicich proved in [Am-Dv] the inequality:

$$h(\alpha) \geq \frac{\log 5}{12} \approx 0.1341$$

(notice that such a result was obtained long time ago as a special case of a more general result, by Schinzel (apply [Sch], Corollary 1', p. 386, to the linear polynomial $P(z) = z - \alpha$), but with the extra assumption $|\alpha| \neq 1$).

The aim of this paper is to generalise both a result of this type and Dobrowolski's result, to obtain:

THEOREM 1.1. *Let $\mathbb{K}$ be any number field and let $\mathbb{L}$ be any abelian extension of $\mathbb{K}$. Then for any nonzero algebraic number α which is not a root of unity, we have*

$$h(\alpha) \geq \frac{C_2(\mathbb{K})}{D} \left(\frac{\log(2D)}{\log\log(5D)} \right)^{-13},$$

where $D = [\mathbb{L}(\alpha) : \mathbb{L}]$ and $C_2(\mathbb{K})$ is a positive constant depending only on $\mathbb{K}$.

This result implies that heights in abelian extensions behave somewhat specially. In this respect, it may not be out of place to recall the following result recently obtained jointly by E. Bombieri and the second author.

Let $\mathbb{K}$ be a number field and consider the compositum $\mathbb{L}$ of all abelian extensions of $\mathbb{K}$ of degree $\leq D$. Then Northcott's theorem (see [No]) *holds in $\mathbb{L}$, that is, for given T, the number of elements of $\mathbb{L}$ with height bounded by T is finite.*

The main ingredients for the proof of Theorem 1.1 (given in Section 5) are a generalisation of Dobrowolski's key inequality (Section 3, Proposition 3.4), which follows as an extension of some ideas from [Am-Dv], and a consequence of the absolute Siegel Lemma of Roy-Thunder-Zhang-Philippon-David (Section 4, Proposition 4.2).

Let $F \in \mathbb{Z}[x_1, \dots, x_n]$ be an irreducible polynomial. Define its Mahler measure as

$$M(F) = \exp\left\{ \frac{1}{(2\pi)^n} \int_0^{2\pi} \cdots \int_0^{2\pi} \log \left| F\left(e^{i\theta_1}, \dots, e^{i\theta_n}\right) \right| d\theta_1 \cdots d\theta_n \right\}.$$

Then it is known (see [Bo], [Law] and [Sm]) that $M(F) = 1$ if and only if F is an extended cyclotomic polynomial, i.e. if and only if

$$F(x_1, \dots, x_n) = x_1^{\lambda_1} \cdots x_n^{\lambda_n} \varphi(x_1^{\mu_1} \cdots x_n^{\mu_n})$$

for some $(\lambda_1, \dots, \lambda_n)$, $(\mu_1, \dots, \mu_n) \in \mathbb{Z}^n$ and for some cyclotomic polynomial $\varphi \in \mathbb{Z}[x]$.

If $n = 1$ and α is a root of F, then $\log M(F) = \deg(F) \cdot h(\alpha)$; hence, if F is not a cyclotomic polynomial,

$$\log M(F) \geq C_1 \left(\frac{\log(3D)}{\log\log(3D)} \right)^{-3}, \qquad D = \deg(F),$$

by the quoted result of Dobrowolski. Recently the first author and S. David ([Am-Da2]) extended this result in several variables. Assume that F is not an extended cyclotomic polynomial. Then, as a special case of Corollaire 1.8 of [Am-Da2],

$$\log M(F) \geq \frac{1}{C_3(n+1)^{1+4/n}n^2} \cdot \left(\frac{\log((n+1)D)}{\log\big((n+1)\log((n+1)D)\big)} \right)^{-3},$$

where C_3 is a positive absolute constant and $D = \deg(F)$.

Using Theorem 1.1 and a density result from [Am-Da2], we can now prove (see Section 6):

COROLLARY 1.2. *Let $F \in \mathbb{Z}[x_1, \dots, x_n]$ be an irreducible polynomial. Assume that F is not an extended cyclotomic polynomial and that $d = \min_{j=1,\dots,n} \deg_{x_j}(F) \geq 1$. Then*

$$\log M(F) \geq C_2(\mathbb{Q}) \left(\frac{\log(2d)}{\log\log(5d)} \right)^{-13}.$$

This estimate is stronger than the quoted result of [Am-Da2] if at least one of the partial degrees of F is small. We also notice that the constant in Corollary 1.2 does not depend on the dimension n.

2. – Notation and Reductions

Throughout this paper, we denote by ζ_m ($m \geq 3$) a primitive m-th root of unity and by μ the set of all roots of unity. We also fix a number field $\mathbb{K}$ and we denote by P the set of rational primes $p \geq 3$ which split completely in $\mathbb{K}$. For $p \in P$ we choose once and for all a prime ideal π_p of $\mathcal{O}_{\mathbb{K}}$ lying above p and we identify π_p with the corresponding place of $\mathbb{K}$. We normalize the corresponding valuation v so that $|p|_v = p^{-1}$.

Let $\mathbb{L}$ be any abelian extension of $\mathbb{K}$. For a given $p \in P$, we define $e_p(\mathbb{L})$ as the ramification index of π_p in $\mathbb{L}$. Let v be any valuation of $\mathbb{L}$ extending π_p. Since $\mathbb{L}/\mathbb{K}$ is normal, the completion $\mathbb{L}_v$ of $\mathbb{L}$ at v depends only on p. Since p splits completely in $\mathbb{K}$ we also have $\mathbb{K}_{\pi_p} = \mathbb{Q}_p$. Then $\mathbb{L}_v$ is an abelian extension of $\mathbb{Q}_p$ and so $\mathbb{L}_v$ is contained in a cyclotomic extension of $\mathbb{Q}_p$ (see e.g. [Wa], p. 320, Theorem 14.2), which we denote by $\mathbb{Q}_p(\zeta_m)$. We take $m = m_p(\mathbb{L})$ to be minimal with this property and we define $e'_p(\mathbb{L})$ as the maximal power

of p dividing m. We remark that $e'_p(\mathbb{L}) = 1$ for all but finitely many $p \in P$ (if π_p does not ramify in $\mathbb{L}$, then $\mathbb{L}_v \subseteq \mathbb{Q}_p(\zeta_m)$ for some integer m with $p \nmid m$: see [Wa], p. 321, Lemma 14.4 (a)). We also define

$$e'(\mathbb{L}) := \sum_{p \in P} (e'_p(\mathbb{L}) - 1)\,.$$

We note that if $\mathbb{L}' \subseteq \mathbb{L}$ are abelian extensions of $\mathbb{K}$, then $e'(\mathbb{L}') \leq e'(\mathbb{L})$.

From now on we let $C_2(\mathbb{K})$ be a positive real number sufficiently small to justify the subsequent arguments.

Let $\mathbb{L}$ be an abelian extension of $\mathbb{K}$ and let $\alpha \notin \mu$ be a nonzero algebraic number which contradicts Theorem 1.1:

$$h(\alpha) < \frac{C_2(\mathbb{K})}{D} \left(\frac{\log(2D)}{\log\log(5D)} \right)^{-13}, \tag{2.1}$$

where $D = [\mathbb{L}(\alpha) : \mathbb{L}]$. We may assume that D is minimal with this property, i.e. that for any $\beta \notin \mu$ of degree $D' < D$ over an abelian extension of $\mathbb{K}$, we have:

$$h(\beta) \geq \frac{C_2(\mathbb{K})}{D'} \left(\frac{\log(2D')}{\log\log(5D')} \right)^{-13}. \tag{2.2}$$

Notice that $t \mapsto t \cdot \big(\log(2t)/\log\log(5t)\big)^{13}$ is an increasing function on $[1, +\infty)$ and that the Weil height is invariant by multiplication by roots of unity. Hence (2.1) and (2.2) imply that:

(2.3) $[\mathbb{L}'(\zeta\alpha) : \mathbb{L}'] \geq D$ for any $\zeta \in \mu$ and for any abelian extension $\mathbb{L}'/\mathbb{K}$

Let $\mathcal{A}$ be the set of abelian extensions $\mathbb{L}/\mathbb{K}$ such that $[\mathbb{L}(\zeta\alpha) : \mathbb{L}] \leq D$ for some $\zeta \in \mu$. We define

$$e' := \min_{\mathbb{L} \in \mathcal{A}} e'(\mathbb{L})\,. \tag{2.4}$$

Replacing if necessary α by $\zeta\alpha$ for some $\zeta \in \mu$ and $\mathbb{L}$ by $\mathbb{L} \cap \mathbb{K}(\alpha)$, we may assume that there exists an abelian extension $\mathbb{L}/\mathbb{K}$ contained in $\mathbb{K}(\alpha)$ satisfying the following properties:

(2.5) $[\mathbb{L}(\alpha) : \mathbb{L}] = D$,

(2.6) $e'(\mathbb{L}) = e'$,

(2.7) for any $\zeta \in \mu$ such that $\mathbb{K}(\zeta\alpha) \subseteq \mathbb{K}(\alpha)$ we have $\mathbb{K}(\zeta\alpha) = \mathbb{K}(\alpha)$.

Since $\mathbb{K} \subset \mathbb{L} \subset \mathbb{K}(\alpha)$, we also have

$$\mathbb{K}(\alpha) = \mathbb{L}(\alpha) \tag{2.8}$$

From now on we fix once and for all an algebraic number α and an abelian extension $\mathbb{L}/\mathbb{K}$ contained in $\mathbb{K}(\alpha)$ which satisfy (2.1), (2.2), (2.3), (2.5), (2.6), (2.7), *and* (2.8). *We also put $e_p = e_p(\mathbb{L})$ for $p \in P$.*

The following lemma will be used several times in the next section.

LEMMA 2.1.

i) *For any integer n we have* $\mathbb{L}(\alpha^n) = \mathbb{L}(\alpha)$.

ii) *For any integer n such that* $\gcd(n, [\mathbb{K}(\alpha): \mathbb{K}(\alpha^n)]) = 1$ *we also have* $\mathbb{K}(\alpha^n) = \mathbb{K}(\alpha)$.

PROOF. We shall use an argument from Rausch (see [Ra], Lemma 3). Assume first

$$r := [\mathbb{L}(\alpha) : \mathbb{L}(\alpha^n)] > 1$$

for some $n \in \mathbb{N}$. The minimal polynomial of α over $\mathbb{L}(\alpha^n)$ is a divisor of $x^n - \alpha^n$. Hence its constant term, say $\beta \in \mathbb{L}(\alpha^n)$, can be written as $\zeta\alpha^r$, where ζ is a n-th root of unity. Moreover,

$$D' := [\mathbb{L}(\beta) : \mathbb{L}] \leq [\mathbb{L}(\alpha^n) : \mathbb{L}] < D\,,$$

and $\beta \notin \mu$. Hence, by (2.2),

$$h(\beta) \geq \frac{C_2(\mathbb{K})}{D'} \left(\frac{\log(2D')}{\log\log(5D')} \right)^{-13}.$$

Since $rD' \leq D$ and $t \mapsto \log(2t)/\log\log(5t)$ increases, we deduce that

$$h(\alpha) = \frac{1}{r} h(\beta) \geq \frac{C_2(\mathbb{K})}{D} \left(\frac{\log(2D)}{\log\log(5D)} \right)^{-13},$$

which contradicts (2.1).

Assume now $r := [\mathbb{K}(\alpha) : \mathbb{K}(\alpha^n)] > 1$ and $\gcd(n, r) = 1$. Arguing as before, we find a n-th root ζ such that $\zeta\alpha^r \in \mathbb{K}(\alpha^n)$. By Bézout's identity, there exist λ, $\mu \in \mathbb{Z}$ such that $\lambda n + \mu r = 1$. Hence

$$\zeta^\mu \alpha = \alpha^{\lambda n} \cdot \left(\zeta\alpha^r\right)^\mu \in \mathbb{K}(\alpha^n) \subsetneq \mathbb{K}(\alpha)\,.$$

This contradicts (2.7). □

3. – Congruences

The following two lemmas generalise Lemma 2 of [Am-Dv]. We first prove a result which shall be applied to tamely ramified primes.

LEMMA 3.1. *Let* $p \in P$. *Then there exists* $\Phi_p \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *such that*

$$|\gamma^p - \Phi_p\gamma|_v \leq p^{-1/e_p}$$

for any integer $\gamma \in \mathbb{L}$ *and for any valuation* v *of* $\overline{\mathbb{Q}}$ *extending* π_p.

PROOF. Let $\wp$ be a prime of $\mathbb{L}$ above π_p and let $G' \subseteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ (resp. $I \subseteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$) be the decomposition (resp. inertia) group of $\wp \mid \pi_p$. Since G'/I is isomorphic to the Galois group of the residue field extension $(O_{\mathbb{L}}/\wp)/(O_{\mathbb{K}}/\pi_p)$, there exists $\Phi_p \in G'$ such that

$$\gamma^p \equiv \Phi_p \gamma \pmod{\wp},$$

for all integers $\gamma \in \mathbb{L}$. Let $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Putting $\sigma^{-1}\gamma$ in place of γ in this congruence and applying σ we get

$$\gamma^p \equiv \sigma \Phi_p \sigma^{-1} \gamma \pmod{\sigma\wp}.$$

On the other hand $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is abelian, and therefore the first displayed congruence holds modulo each prime of $\mathbb{L}$ lying over π_p. Lemma 3.1 follows. □

We now consider primes having a large ramification index.

LEMMA 3.2. *Let $p \in P$. Then there exists a subgroup H_p of* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *of order*

$$o(H_p) \geq \min\{e_p, p\}$$

such that

$$|\gamma^p - \sigma\gamma^p|_v \leq p^{-1}$$

for any integer $\gamma \in \mathbb{L}$, for any $\sigma \in H_p$ and for any valuation v of $\mathbb{L}$ extending π_p.

Moreover, for any extension $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ of $\sigma \in H_p \backslash \{\mathrm{Id}\}$, we have $\tau\alpha^p \neq \alpha^p$.

PROOF. Let v be any valuation of $\mathbb{L}$ extending π_p, let L_v be the completion of $\mathbb{L}$ at v (we recall that L_v depends only on p) and let $m = m_p(\mathbb{L})$ be the smallest positive integer such that $\mathbb{L}_v \subseteq \mathbb{Q}_p(\zeta_m)$. We decompose m as $m = q \cdot n$ where $q = e'_p(\mathbb{L})$ is the maximal power of p dividing m.

If π_p does not ramify in $\mathbb{L}$ the lemma is trivial (we have $e_p = 1$ and we take $H_p = \{\mathrm{Id}\}$). Therefore we assume that π_p ramifies in $\mathbb{L}$, whence *a fortiori* in $\mathbb{Q}_p(\zeta_m)$. This implies that $p|q$. Let Σ_p be the Galois group of $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p})$. Then Σ_p is cyclic of order p or $p-1$ depending on whether $p^2|q$ or not. By the minimality property of m we have that Σ_p does not fix $\mathbb{L}_v$, and hence induces by restriction a nontrivial subgroup H_v^* of $\mathrm{Gal}(\mathbb{L}_v/\mathbb{K}_{\pi_p})$. Note that if $p^2 \nmid q$, the order of H_v^* is at least e_p (since $\mathbb{Q}_p(\zeta_{m/p})/\mathbb{Q}_p$ is unramified), while if $p^2 \mid q$, necessarily H_v^* has order p.

We define H_v to be the (isomorphic) image of H_v^* in $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. If v' is another valuation of $\mathbb{L}$ extending π_p, we have $v' = \tau v$ for some $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ and the embedding of $\mathbb{L}$ in $\mathbb{L}_{v'}$ is obtained by composing τ with the embedding of $\mathbb{L}$ in $\mathbb{L}_v$. We thus see that $\mathbb{L}_{v'} = \mathbb{L}_v$, and so the group H_v^* does not depend on v. The same argument shows that $H_{v'} = \tau^{-1} H_v \tau$. Therefore, since $\mathbb{L}/\mathbb{K}$ is abelian, we have $H_v = H_{v'}$. Hence this group depends only on p, and we denote it by H_p. By the previous arguments we have:

$$\begin{cases} o(H_p) \geq e_p \text{ and } o(H_p) \mid o(\Sigma_p) = p-1, & \text{if } p^2 \nmid q\,; \\ o(H_p) = o(\Sigma_p) = p, & \text{if } p^2 \mid q\,. \end{cases} \tag{3.1}$$

Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}_p(\zeta_m)$. To prove that $|\gamma^p - \sigma\gamma^p|_v \leq p^{-1}$ for any integer $\gamma \in \mathbb{L}$, it suffices to verify the congruence

$$\gamma^p \equiv \sigma\gamma^p \pmod{\pi_p\mathcal{O}}$$

for every $\gamma \in \mathcal{O}$ and $\sigma \in \Sigma_p$. In fact, if this is true we have in particular that, for all integers $\gamma \in \mathbb{L}$ and for all $\sigma \in H_p$, the integer $\gamma^p - \sigma\gamma^p \in \mathbb{L}$ has order $\geq e_p$ at v, whence the assertion.

To prove the last displayed congruence, recall the well-known equality $\mathcal{O} = \mathbb{Z}_p[\zeta_m]$. Put then $\gamma = f(\zeta_m)$, where $f \in \mathbb{Z}_p[X]$. Let $\sigma \in H_p$; since σ fixes $\mathbb{Q}_p(\zeta_{m/p})$ we have $\sigma\zeta_m^p = \zeta_m^p$. Combining these facts with Fermat's little theorem we find

$$\sigma\gamma^p = \sigma f(\zeta_m)^p \equiv \sigma f(\zeta_m^p) = f(\zeta_m^p) \equiv \gamma^p \pmod{p\mathcal{O}},$$

as required.

We now prove the last statement of the lemma. Let $\sigma \in H_p$, $\sigma \neq \mathrm{Id}$ and let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ be any extension of σ. Assume $\tau\alpha^p = \alpha^p$ and denote by $\mathbb{E}$ the subfield of $\mathbb{L}$ fixed by σ. We notice that the minimal polynomial of α^p over $\mathbb{L}$ has coefficients in $\mathbb{E}$. Moreover $\mathbb{L}(\alpha^p) = \mathbb{L}(\alpha)$ by Lemma 2.1 i). Hence

$$[\mathbb{E}(\alpha^p) : \mathbb{E}] = [\mathbb{L}(\alpha^p) : \mathbb{L}] = [\mathbb{L}(\alpha) : \mathbb{L}] = D. \tag{3.2}$$

We quote the following sublemma:

SUBLEMMA.

$$o(\Sigma_p) = p.$$

PROOF. Since $\mathbb{E} \subsetneq \mathbb{L}$, we have $[\mathbb{L}(\alpha) : \mathbb{E}] > [\mathbb{L}(\alpha) : \mathbb{L}]$. Therefore, by (3.2),

$$[\mathbb{L}(\alpha) : \mathbb{E}(\alpha^p)] > 1. \tag{3.3}$$

Remark that $\mathbb{K}(\alpha) = \mathbb{L}(\alpha)$ (see (2.8)) and $\mathbb{K} \subseteq \mathbb{E}(\alpha^p) \subseteq \mathbb{L}(\alpha)$. Hence $[\mathbb{L}(\alpha) : \mathbb{E}(\alpha^p)]$ divides $[\mathbb{K}(\alpha) : \mathbb{K}(\alpha^p)]$. If we had $\mathbb{K}(\alpha) = \mathbb{K}(\alpha^p)$, then τ would fix $\mathbb{K}(\alpha) = \mathbb{L}(\alpha)$, hence *a fortiori* $\mathbb{L}$. Therefore $\mathbb{K}(\alpha) \neq \mathbb{K}(\alpha^p)$, and, by Lemma 2.1 ii), $[\mathbb{K}(\alpha) : \mathbb{K}(\alpha^p)] = p$. We infer that

$$[\mathbb{L}(\alpha) : \mathbb{E}(\alpha^p)] \mid p$$

and, by (3.3), $[\mathbb{L}(\alpha) : \mathbb{E}(\alpha^p)] = p$. Since the field extension $\mathbb{E} \subseteq \mathbb{L}$ is Galois, $[\mathbb{L}(\alpha) : \mathbb{E}(\alpha^p)]$ divides $[\mathbb{L} : \mathbb{E}]$ which is $\leq p$. Therefore

$$o(H_p) = [\mathbb{L} : \mathbb{E}] = p$$

and, by (3.1), $|\Sigma_p| = p$, as claimed. □

Let now fix the (primitive) q-th root of unity $\zeta_q = \zeta_m^n$. Since $\mathbb{L}_v(\zeta_q) \subseteq \mathbb{Q}_p(\zeta_m)$, the Galois group Σ_p induces by restriction a nontrivial subgroup of $\mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{K})$, which is necessarily cyclic of order p by the sublemma. Let $\mathbb{F} \subseteq \mathbb{L}(\zeta_q)$ be its fixed field and let ρ be a generator of $\mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{F})$. Then

$$\mathbb{F} \supseteq \mathbb{E} \tag{3.4}$$

and

$$\rho\zeta_q = \zeta_p\zeta_q \tag{3.5}$$

for some primitive p-th root of unity ζ_p (recall that $p \nmid n$).

We claim that there exists an integer u such that $\zeta_q^{-u}\alpha \in \mathbb{F}(\alpha^p)$. We may assume $\alpha \notin \mathbb{F}(\alpha^p)$, otherwise our claim is trivial; hence *a fortiori* $\mathbb{F}(\alpha^p) \subsetneqq \mathbb{L}(\zeta_q, \alpha)$. Moreover, by Galois theory, $[\mathbb{L}(\zeta_q, \alpha^p) : \mathbb{F}(\alpha^p)]$ divides $[\mathbb{L}(\zeta_q) : \mathbb{F}] = p$ and $\mathbb{L}(\zeta_q, \alpha^p) = \mathbb{L}(\zeta_q, \alpha)$ by Lemma 2.1 i). Hence $[\mathbb{L}(\zeta_q, \alpha) : \mathbb{F}(\alpha^p)] = p$ and, again by Galois theory, the restriction

$$r : \mathrm{Gal}(\mathbb{L}(\zeta_q, \alpha)/\mathbb{F}(\alpha^p)) \to \mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{F})$$

is a group isomorphism. Let $\tilde{\rho}$ be a generator of $\mathrm{Gal}(\mathbb{L}(\zeta_q, \alpha)/\mathbb{F}(\alpha^p))$. Then, by (3.5),

$$\tilde{\rho}\zeta_q = \zeta_p\zeta_q \quad \text{and} \quad \tilde{\rho}\alpha = \zeta_p^u\alpha$$

for some $u \in \mathbb{N}$. Hence $\zeta_q^{-u}\alpha$ is left fixed by $\tilde{\rho}$ and so belongs to $\mathbb{F}(\alpha^p)$, as claimed.

By (3.2) and (3.4) we have

$$[\mathbb{F}(\zeta_q^{-u}\alpha) : \mathbb{F}] \le [\mathbb{F}(\alpha^p) : \mathbb{F}] \le [\mathbb{E}(\alpha^p) : \mathbb{E}] = D\,.$$

Since $\mathbb{F}_v \subseteq \mathbb{Q}_p(\zeta_{m/p})$ and $\mathbb{F} \subseteq \mathbb{L}(\zeta_q)$, we also have

$$\begin{aligned} &e'_p(\mathbb{F}) \le q/p < q = e'_p(\mathbb{L})\,; \\ &e'_l(\mathbb{F}) \le e'_l(\mathbb{L}) \quad \text{for} \quad l \in P,\ l \ne p\,. \end{aligned}$$

Therefore

$$[\mathbb{F}(\zeta_q^{-u}\alpha) : \mathbb{F}] \le D \quad \text{and} \quad e'(\mathbb{F}) < e'(\mathbb{L}) = e'\,,$$

which contradicts the definition (2.4) of e'. □

We shall deduce from the two previous lemmas two propositions which generalise the key argument of [Do]. They will be used to extrapolate in the proof of Theorem 1.1. To do this, we need the following further lemma, which is an easy consequence of the Strong Approximation Theorem.

LEMMA 3.3. *Let $\mathbb{E}$ be any number field and let v be a non-archimedean place of $\mathbb{E}$. Then, for any $\gamma_1, \dots, \gamma_n \in \mathbb{E}$ there exists $\beta \in \mathcal{O}_{\mathbb{E}}$ such that $\beta\gamma_j$ is an algebraic integer for $j = 1, \dots, n$ and*

$$|\beta|_v = \max\{1, |\gamma_1|_v, \dots, |\gamma_n|_v\}^{-1}.$$

PROOF. See [Am-Da1], Lemma 3.2.

PROPOSITION 3.4. *Let L_1 and T_1 be two positive integers. Assume that there exists a polynomial F of degree $\leq L_1$ with algebraic integer coefficients, vanishing at all the conjugates $\alpha_1, \dots, \alpha_D$ of α over $\mathbb{L}$ with multiplicity $\geq T_1$. Let also $p \in P$ and let v be any valuation of $\overline{\mathbb{Q}}$ extending π_p. Then*

$$|F^\tau(\alpha^p)|_v \leq p^{-T_1/e_p} \max\{1, |\alpha|_v\}^{pL_1},$$

for any $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ extending Φ_p.

PROOF. Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ extend Φ_p. We extend v to the field $\overline{\mathbb{Q}}(x)$ in the canonical way (i.e., by setting $|x|_v = 1$). Let $a(x) = a_0 + a_1x + \cdots + a_{D-1}x^{D-1} + x^D$ be the minimal polynomial of α over $\mathbb{L}$. By Lemma 3.3, there exists $\beta \in \mathcal{O}_{\mathbb{L}}$ such that

$$(f_0, \dots, f_D) := (\beta a_0, \dots, \beta a_{D-1}, \beta) \in \mathcal{O}_{\mathbb{L}}^{D+1}$$

and $\max_j\{|\tau f_j|_v\} = 1$. Therefore

$$f(x) = f_0 + f_1x + \cdots + f_Dx^D \in \mathcal{O}_{\mathbb{L}}[x]$$

and $|f^\tau|_v = 1$. Using Fermat's little theorem and Lemma 3.1 we find that

$$|f(x)^p - f^\tau(x^p)|_v \leq p^{-1/e_p}.$$

Again by Lemma 3.3, there exists an algebraic integer $\beta' \in \mathbb{K}(\alpha)$ such that $\beta'\alpha$ is also integer and $|\beta'|_v = \max\{1, |\alpha|_v\}^{-1}$. We have

$$|\beta'^{pD} f^\tau(\alpha^p)|_v = |\beta'^{pD} f(\alpha)^p - \beta'^{pD} f^\tau(\alpha^p)|_v \leq p^{-1/e_p}.$$

Hence

$$|f^\tau(\alpha^p)|_v \leq p^{-1/e_p} \max\{1, |\alpha|_v\}^{pD}.$$

Since F has algebraic integer coefficients and since $|f^\tau|_v = 1$, by Gauss' lemma we have the factorisation $F = q \cdot f^{T_1}$ with $|q^\tau|_v \leq 1$. Hence

$$|F^\tau(\alpha^p)|_v \leq p^{-T_1/e_p} \max\{1, |\alpha|_v\}^{pL_1}$$

as claimed. □

PROPOSITION 3.5. *Let p, v and $\alpha_1, \dots, \alpha_D$ be as in Proposition* 3.4. *Let L_2 and T_2 be two positive integers. Assume that there exists a polynomial F of degree $\leq L_2$ with algebraic integer coefficients vanishing at $\alpha_1^p, \dots, \alpha_D^p$ with multiplicity $\geq T_2$. Then*

$$|F^\tau(\alpha^p)|_v \leq p^{-T_2} \max\{1, |\alpha|_v\}^{pL_2},$$

for any $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ such that $\tau_{|\mathbb{L}} \in H_p$.

PROOF. Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ be such that $\tau_{|\mathbb{L}} \in H_p$. As in the proof of Proposition 3.4, we extend v to the field $\overline{\mathbb{Q}}(x)$ in the canonical way and we select a multiple

$$f(x) = f_0 + f_1 x + \cdots + f_D x^D$$

of the minimal polynomial of α over $\mathbb{L}$, such that $f \in \mathcal{O}_{\mathbb{L}}$ and $|f^\tau|_v = 1$. Let $g(x) = g_0 + g_1 x + \cdots + g_D x^D$ be the polynomial obtained by multiplying the minimal polynomial of α^p over $\mathbb{L}$ by f_D^p. Then again $g \in \mathcal{O}_{\mathbb{L}}[x]$ and $|g^\tau|_v = 1$. Moreover, g is irreducible by Lemma 2.1 i). Using Fermat's little theorem we find that

$$|g_j - f_j^p|_v \leq p^{-1} \quad \text{and} \quad |\tau g_j - \tau f_j^p|_v \leq p^{-1},$$

for $j = 0, \dots, D$. Moreover, by Lemma 3.2,

$$|f_j^p - \tau f_j^p|_v \leq p^{-1}, \qquad j = 0, \dots, D.$$

Therefore

$$|g(x) - g^\tau(x)|_v \leq p^{-1}.$$

As in the proof of Proposition 3.4, we deduce that

$$|g^\tau(\alpha^p)|_v \leq p^{-1} \max\{1, |\alpha|_v\}^{pD}$$

and

$$|F^\tau(\alpha^p)|_v \leq p^{-T_2} \max\{1, |\alpha|_v\}^{pL_2},$$

as claimed. □

4. – The Absolute Siegel Lemma

Let $S \subseteq \overline{\mathbb{Q}}^n$ be a vector subspace of dimension d. Following Schmidt [Schm], Chapter 1, Section 8, we define the height $h_2(S)$ as

$$h_2(S) = \sum_v \frac{[\mathbb{F}_v : \mathbb{Q}_v]}{[\mathbb{F} : \mathbb{Q}]} \log \|\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_d\|_v.$$

In this formula $\mathbf{x}_1, \dots, \mathbf{x}_n$ denotes any basis of V over the ground field, $\mathbb{F}$ is a number field containing the coordinates of the vectors $\mathbf{x}_j$, and $\|\cdot\|_v$ is the

sup norm if v is finite and the euclidean norm if v is archimedean (we endow $\wedge^d \overline{\mathbb{Q}}^n$ with the standard coordinates and the induced euclidean metric). Let $\alpha \in \overline{\mathbb{Q}}^n$ and let S be the one-dimensional subspace generated by it. By abuse of notation, we put $h_2(\alpha) = h_2(S)$.

The following result improves the main result of D. Roy and J. Thunder (see [Ro-Th], Theorem 2.2). It is a consequence of Theorem 5.2 of [Zh] and is proved in [Da-Ph] (see Lemma 4.7 and the remark which follows it).

LEMMA 4.1. *For any $\varepsilon > 0$ there exists a nonzero vector $\mathbf{x} \in S$ such that*

$$h_2(\mathbf{x}) \leq \frac{h_2(S)}{d} + \frac{\log d}{2} + \varepsilon .$$

As an immediate consequence, we find:

PROPOSITION 4.2. *Let $\beta_1, \dots, \beta_k$ be distinct algebraic numbers and L, T two positive integers with $L > kT$. Then there exists a nonzero polynomial F with algebraic integer coefficients, of degree $< L$, vanishing at $\beta_1, \dots, \beta_k$ with multiplicity $\geq T$, such that:*

$$h_2(F) \leq \frac{kT}{L-kT} \left\{ (T+1/2)\log L + \frac{L}{k}\sum_{j=1}^{k} h(\beta_j) \right\} + \frac{1}{2}\log L .$$

PROOF. Let us consider the vectors:

$$\mathbf{y}_{j,\lambda} = \left(0, \dots, 0, 1, \binom{\lambda+1}{\lambda}\beta_j, \dots, \binom{L-1}{\lambda}\beta_j^{L-1-\lambda}\right) \in \overline{\mathbb{Q}}^L$$

($j = 1, \dots, k$; $\lambda = 0, \dots, T-1$). Using the inequality $\sum_{\mu=\lambda}^{L-1} \binom{\mu}{\lambda}^2 \leq L^{2T+1}$, we easily obtain

$$\|\mathbf{y}_{j,\lambda}\|_v \leq \begin{cases} \max\{1, |\beta_j|_v\}^L, & \text{if } v \nmid \infty ; \\ L^{T+1/2}\max\{1, |\beta_j|_v\}^L, & \text{if } v \mid \infty . \end{cases}$$

Hence $h_2(\mathbf{y}_{j,\lambda}) \leq (T+1/2)\log L + Lh(\beta_j)$. The vector subspace

$$S = \{\mathbf{x} \in \overline{\mathbb{Q}}^L \mid \mathbf{y}_{j,\lambda} \cdot \mathbf{x} = 0, \quad \text{for} \quad j = 1, \dots, k \quad \text{and} \quad \lambda = 0, \dots, T-1\}$$

has dimension $d = L - kT$ and the vectors $\mathbf{y}_{j,\lambda}$ are a basis of its orthogonal complement $S^\perp$. From [Schm], Chapter 1, Section 8 we have

$$h_2(S) = h_2(S^\perp) \leq \sum_{j,\lambda} h_2(\mathbf{y}_{j,\lambda}) \leq kT(T+1/2)\log L + T\sum_{j=1}^{k} h(\beta_j) .$$

We now apply Proposition 4.2, taking $\varepsilon = \frac{1}{2}\log\frac{L}{L-kT}$. □

5. – Proof of the Main Result

In the sequel we denote by $c_1, c_2, \dots, c_{16}$ positive constants depending only on the ground field $\mathbb{K}$. We also denote by C a positive, sufficiently large constant, chosen so that the inequalities below will be satisfied. We fix two parameters:

$$N = C^9 \frac{(\log(2D))^6}{(\log\log(5D))^5} \quad \text{and} \quad E = C^3 \left(\frac{\log(2D)}{\log\log(5D)}\right)^2 .$$

Let Λ be the set of rational primes $p \in P$ such that $c_1 N \le p \le N$. If c_1 is sufficiently small we have, by the Chebotarev Theorem,

$$|\Lambda| \ge \frac{c_2}{\log C} \cdot \frac{N}{\log\log(5D)} .$$

Let Λ_1 be the subset of primes $p \in \Lambda$ such that $e_p \le E$ and let Λ_2 be its complement in Λ, i.e. the subset of primes $p \in \Lambda$ such that $e_p > E$. We distinguish two cases.

- First Case: $|\Lambda_1| \ge \dfrac{c_2}{2\log C} \cdot \dfrac{N}{\log\log(5D)}$.

We introduce two other parameters:

$$L_1 = \left[C^8 D \left(\frac{\log(2D)}{\log\log(5D)}\right)^6\right] \quad \text{and} \quad T_1 = \left[C^4 \left(\frac{\log(2D)}{\log\log(5D)}\right)^3\right] .$$

Using the absolute Siegel lemma (Proposition 4.2) we find a nonzero polynomial F with algebraic integer coefficients, of degree $< L_1$, vanishing at $\alpha_1, \dots, \alpha_D$ with multiplicity $\ge T_1$, such that:

$$\begin{aligned} h_2(F) &\le \frac{DT_1}{L_1 - DT_1}\{(T_1 + 1/2)\log(L_1+1) + L_1 h(\alpha)\} + \frac{1}{2}\log L_1 \\ &\le c_3 \log C \cdot \log(2D) + c_4 C^4 D \left(\frac{\log(2D)}{\log\log(5D)}\right)^3 h(\alpha) . \end{aligned}$$

Using the upper bound (2.1) for $h(\alpha)$ we obtain

$$\begin{aligned} h_2(F) &\le c_3 \log C \cdot \log(2D) + c_4 C^4 C_2(\mathbb{K}) \left(\frac{\log\log(5D)}{\log(2D)}\right)^{10} \\ &\le c_5 \log C \cdot \log(2D) , \end{aligned} \tag{5.1}$$

if $C_2(\mathbb{K}) \le C^{-4} \log C$.

Suppose that there exist a prime $p \in \Lambda_1$ and $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ extending Φ_p such that $F^\tau(\alpha^p) \ne 0$. Let $\mathbb{F}$ be a field containing the coefficients of F^τ

and α. Using the product formula, Proposition 3.4 and the inequality $e_p \leq E$, we obtain:

$$\begin{aligned} 0 &= \frac{1}{[\mathbb{F}:\mathbb{Q}]} \sum_v [\mathbb{F}_v : \mathbb{Q}_v] \log |F^\tau(\alpha^p)|_v \\ &\leq -\frac{c_6 T_1}{E} \log p + p L_1 h(\alpha) + h_2(F) + \frac{1}{2} \log L_1 . \end{aligned}$$

Therefore, inserting the upper bounds (5.1) for $h_2(F)$ and (2.1) for $h(\alpha)$,

$$\begin{aligned} 0 &\leq -c_7 C \log(2D) + c_8 C^{17} \frac{D(\log(2D))^{12}}{(\log\log(5D))^{11}} h(\alpha) + c_9 \log C \cdot \log(2D) \\ &\leq -c_{10} C \log(2D) + c_8 C^{17} C_2(\mathbb{K}) \frac{\log\log(2D)}{\log(5D)} \end{aligned}$$

Hence, if $C_2(\mathbb{K}) < c_8^{-1} c_{10} C^{-16}$ we have $F(\tau\alpha^p) = 0$ for all primes $p \in \Lambda_1$ and for all $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ extending Φ_p^{-1}.

Let $p \in \Lambda_1$. By Lemma 2.1 i), $[\mathbb{L}(\alpha^p) : \mathbb{L}] = D$. Hence there are exactly D homomorphisms $\tau : \mathbb{L}(\alpha^p) \to \overline{\mathbb{Q}}$ extending Φ_p^{-1}. Moreover, if $p \neq q$ and if $\tau_1, \tau_2 \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$, then $\tau_1\alpha^p \neq \tau_2\alpha^q$ by a lemma of Dobrowolski (see [Do] Lemma 2 i). From these remarks we obtain:

$$L_1 \geq \deg F \geq D|\Lambda_1| \geq \frac{c_2}{2\log C} \cdot \frac{DN}{\log\log(5D)} ,$$

which contradicts our choice of parameters. Theorem 1.1 is proved in the first case.

- Second Case: $|\Lambda_2| > \dfrac{c_2}{2\log C} \cdot \dfrac{N}{\log\log(5D)}$.

We introduce two new parameters:

$$L_2 = \left[C^{11} D \left(\frac{\log(2D)}{\log\log(5D)} \right)^8 \right] \quad \text{and} \quad T_2 = \left[C \frac{\log(2D)}{\log\log(5D)} \right] .$$

Let $\alpha_1, \ldots, \alpha_D$ be the conjugates of α over $\mathbb{L}$. We apply Proposition 4.2 (the absolute Siegel lemma) to the set of algebraic numbers

$$\{\alpha_j^p \quad \text{such that} \quad j = 1, \ldots, D \quad \text{and} \quad p \in \Lambda_2\} .$$

We find a nonzero polynomial F with algebraic integer coefficients, of degree $< L_2$, vanishing at $\alpha_1^p, \ldots, \alpha_D^p$ with multiplicity $\geq T_2$ for all $p \in \Lambda_2$, such that:

$$\begin{aligned} h_2(F) &\leq \frac{DT_2|\Lambda_2|}{L_2 - DT_2|\Lambda_2|} \{(T_2+1)\log(L_2 + 1/2) + L_2 N h(\alpha)\} + \frac{1}{2}\log L_2 \\ &\leq c_{11} \log C \cdot \log(2D) + c_{12} C^{19} D \frac{(\log(2D))^{13}}{(\log\log(5D))^{12}} h(\alpha) . \end{aligned}$$

From the upper bound (2.1) for $h(\alpha)$ we obtain:

$$h_2(F) \leq c_{11} \log C \cdot \log(2D) + c_{12} C^{19} C_2(\mathbb{K}) \log\log(5D) \leq c_{13} \log C \cdot \log(2D),$$

if $C_2(\mathbb{K}) \leq C^{-19} \log C$.

Suppose that there exist a prime $p \in \Lambda_2$ and $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ such that $\tau_{|\mathbb{L}} \in H_p$ and $F^\tau(\alpha^p) \neq 0$. As before, let $\mathbb{F}$ be a field containing the coefficients of F^τ and α. Using the product formula, Proposition 3.5 and the upper bounds for $h(\alpha)$ and $h_2(F)$, we obtain:

$$\begin{aligned} 0 &= \frac{1}{[\mathbb{F}:\mathbb{Q}]} \sum_v [\mathbb{F}_v : \mathbb{Q}_v] \log |F^\tau(\alpha^p)|_v \\ &\leq -c_{14} T_2 \log p + p L_2 h(\alpha) + h_2(F) + \frac{1}{2} \log L_2 \\ &\leq -c_{15} C \log(2D) + c_{16} C^{20} C_2(\mathbb{K}) \log\log(5D) \end{aligned}$$

Hence, if $C_2(\mathbb{K}) < c_{15}^{-1} c_{16} C^{-19}$ we have $F(\tau\alpha^p) = 0$ for all primes $p \in \Lambda_2$ and for all $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ such that $\tau_{|\mathbb{L}} \in H_p$.

Let $p \in \Lambda_2$ and let $\sigma \in H_p$. By Lemma 2.1 i), $[\mathbb{L}(\alpha^p) : \mathbb{L}] = D$. Hence there are exactly D homomorphisms $\tau : \mathbb{L}(\alpha^p) \to \overline{\mathbb{Q}}$ extending σ. Let $\tilde{\sigma} \in H_p \backslash \{\sigma\}$ and let τ, $\tilde{\tau} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ extend σ and $\tilde{\sigma}$ respectively. Then, by the last statement of Lemma 3.2, $\tau\alpha^p \neq \tilde{\tau}\alpha^p$. Moreover, if $p \neq q$ and if τ_1, $\tau_2 \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$, then $\tau_1\alpha^p \neq \tau_2\alpha^q$ by the quoted lemma of Dobrowolski ([Do] Lemma 2 i). From these remarks and from the inequalities $e_p \geq E$ and $p \geq c_1 N \geq E$ $(p \in P)$ we obtain:

$$L_2 \geq \deg F \geq \sum_{p \in \Lambda_2} D|H_p| \geq \sum_{p \in \Lambda_2} D \min\{e_p, p\} \geq |\Lambda_2| DE \geq \frac{c_2}{2 \log C} \cdot \frac{DNE}{\log\log(5D)}$$

which contradicts again our choice of parameters. The proof of Theorem 1.1 is now complete.

6. – Proof of Corollary 1.1

We may assume $d = \deg_{x_n}(F) \geq 1$. Let $\varepsilon > 0$. Then, by Proposition 2.7 of [Am-Da2], the set of algebraic points $(\omega_1, \dots, \omega_{n-1}, \alpha)$ such that $\omega_1, \dots, \omega_{n-1} \in \boldsymbol{\mu}$, $\alpha \neq 0$,

$$h(\alpha) \leq \frac{\log M(F)}{d} + \varepsilon$$

and $F(\omega_1, \dots, \omega_{n-1}, \alpha) = 0$, is Zariski-dense in the hypersurface $V \subseteq \mathbb{G}_{\mathrm{m}}^n$ defined by $F = 0$. Since F is not an extended cyclotomic polynomial, V is

not a union of translates of subgroups by torsion points. Hence, by a result of M. Laurent (see [Lau]), $\mu^n \cap V$ is not Zariski-dense in V. This implies that there exist $\omega_1, \dots, \omega_{n-1} \in \mu$ and $\alpha \in \overline{\mathbb{Q}}^* \backslash \mu$ such that

$$h(\alpha) \leq \frac{\log M(F)}{d} + \varepsilon$$

and

$$[\mathbb{Q}(\omega_1, \dots, \omega_{n-1}, \alpha) : \mathbb{Q}(\omega_1, \dots, \omega_{n-1})] \leq d .$$

Applying Theorem 1.1 with $\mathbb{K} = \mathbb{Q}$ and $\mathbb{L} = \mathbb{Q}(\omega_1, \dots, \omega_{n-1})$, we obtain:

$$\frac{\log M(F)}{d} + \varepsilon \geq h(\alpha) \geq \frac{C_2(\mathbb{Q})}{d} \left(\frac{\log\log(5d)}{\log(2d)} \right)^{13} .$$

Corollary 1.1 easily follows. □

ADDED IN PROOF. The main result of the present paper can be slightly improved if the number of rational primes ramified in the abelian extension is small. We have:

THEOREM 1.1.BIS. *Let $\mathbb{K}$ be any number field and let $\mathbb{L}$ be any abelian extension of $\mathbb{K}$. Let also α be a nonzero algebraic number which is not a root of unity and put $D = [\mathbb{L}(\alpha) : \mathbb{L}]$. Assume that the number of rational primes ramified in $\mathbb{L}$ is bounded by $c_0(\frac{\log(2D)}{\log\log(5D)})^2$ for some positive constant c_0. Then*

$$h(\alpha) \geq \frac{C_2(\mathbb{K}, c_0)}{D} \left(\frac{\log(2D)}{\log\log(5D)} \right)^{-3} ,$$

where $C_2(\mathbb{K}, c_0)$ is a positive constant depending only on $\mathbb{K}$ and c_0.

PROOF. Assume that the conclusion of Theorem 1.1 bis is false. Then, in Section 2, we can choose an abelian extension $\mathbb{L}$ and an algebraic number α satisfying (2.1), (2.2) (with the exponent -13 replaced by -3 and $C_2(\mathbb{K})$ replaced by $C_2(\mathbb{K}, c_0)$), (2.3), (2.5), (2.6), (2.7), and (2.8). We choose in Section 5, the parameters $N = C^3 \frac{(\log(2D))^2}{(\log\log(5D))}$ and $E = 1$ and we remark that the set Λ_1 of rational primes $p \in P$ such that $c_1 N \leq p \leq N$ and $e_p = 1$ has cardinality $\geq \frac{c_2}{\log C} \cdot \frac{N}{\log\log(5D)}$, by the Chebotarev Theorem and by the extra assumption of Theorem 1.1 bis. As in Section 5, we introduce two other parameters:

$$L_1 = \left[C^2 D \left(\frac{\log(2D)}{\log\log(5D)} \right)^2 \right] \quad \text{and} \quad T_1 = \left[C \frac{\log(2D)}{\log\log(5D)} \right] .$$

The same arguments show that there exists a nonzero polynomial F with algebraic integer coefficients, of degree $< L_1$, vanishing at $\tau\alpha^p$ for all primes $p \in \Lambda_1$ and for all $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ extending Φ_p^{-1}. As in the original proof, we deduce that

$$L_1 \geq \deg F \geq D|\Lambda_1| \geq \frac{c_2}{\log C} \cdot \frac{DN}{\log\log(5D)},$$

which contradicts our choice of parameters. Theorem 1.1 bis is proved. □

Theorem 1.1 bis allows us to improve Corollary 1.2:

COROLLARY 1.2 BIS. *Let $F \in \mathbb{Z}[x_1, \dots, x_n]$ be an irreducible polynomial. Assume that F is not an extended cyclotomic polynomial and that $d = \min_{j=1,\dots,n} \deg_{x_j}(F) \geq 1$. Then*

$$\log M(F) \geq C_2(\mathbb{Q}, 1) \left(\frac{\log(2d)}{\log\log(5d)} \right)^{-3}.$$

PROOF. Let $\tilde{\mu}$ be the union of the sets of primitive p-roots of unity, p being an arbitrary prime number. We remark that, by Proposition 2.7 of [Am-Da2], the set of algebraic points $(\omega_1, \dots, \omega_{n-1}, \alpha)$ such that $\omega_1, \dots, \omega_{n-1} \in \tilde{\mu}$, $\alpha \neq 0$, $h(\alpha) \leq \frac{\log M(F)}{d} + \varepsilon$ and $F(\omega_1, \dots, \omega_{n-1}, \alpha) = 0$, is Zariski-dense in the hypersurface $V = \{F = 0\} \subseteq \mathbb{G}_{\mathrm{m}}^n$. The sequel of the proof is the same as in Section 6, but we apply Theorem 1.1 bis instead of Theorem 1.1.

REFERENCES

[Am-Da1] F. AMOROSO – S. DAVID, *Le problème de Lehmer en dimension supérieure*, J. reine angew. Math. **513** (1999), 145-179.

[Am-Da2] F. AMOROSO – S. DAVID, *Minoration de la hauteur normalisée des hypersurfaces*, Acta Arith. **92** (2000), no. 4, 340-366.

[Am-Dv] F. AMOROSO – R. DVORNICICH, *A lower bound for the height in Abelian extensions*, J. Number Theory **80** (2000), no. 2, 260-272.

[Bo] D. BOYD, *Kronecker's theorem and Lehmer's problem for polynomials in several variables*, J. Number Theory **13** (1980), 116-121.

[Da-Ph] P. PHILIPPON – S. DAVID, *Minorations des hauteurs normalisées des sous-variétés des tores*, Ann. Scuola Norm. Sup. Pisa a. Sci (4) **28** (1999), 489-543.

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

[Lau] M. LAURENT, *Equations diophantiennes exponentielles*, Invent. Math. **78** (1984), 299-327.

[Law] W. LAWTON, *A generalization of a theorem of Kronecker*, J. of the Science Faculty of Chiangmai University (Thailand) **4** (1977), 15-23.

[Le] D. H. LEHMER, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461-479.

[Na] W. NARKIEWICZ, "Elementary and analytic theory of algebraic numbers", Second edition, Springer-Verlag, Berlin, PWN-Polish Scientific Publishers, Warsaw, 1990.

[No] N. NORTHCOTT, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Camb. Philos. Soc. **45** (1949), 502-509.

[Ra] U. RAUSCH, *On a theorem of Dobrowolski about the product of conjugate numbers*, Colloq. Math. **50** (1985), no. 1, 137-142.

[Ro-Th] D. ROY – J. THUNDER, *An absolute Siegel's lemma*, J. reine angew. Math. **476** (1996), 1-12.

[Schi] A. SCHINZEL, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385-399. Addendum, ibid. **26** (1973), 329-361.

[Schm] W. M. SCHMIDT, "Diophantine approximations and Diophantine equations", Lecture Notes in Mathematics **1467**, Springer-Verlag, Berlin, 1991.

[Sm] C. J. SMYTH, *A Kronecker-type theorem for complex polynomials in several variables*, Canad. Math. Bull. **24** (1981), 447-452. Errata, ibid. **25** (1982), 504.

[Wa] L. C. WASHINGTON, "Introduction to Cyclotomic Fields", Springer-Verlag, New York, 1982.

[Zh] S. ZHANG, *Positive line bundles on arithmetic surfaces*, Ann. of Math. **136** (1992), 569-587.

Département de Mathématiques
Université de Caen
Campus II, BP 5186
4032 Caen Cédex, France
amoroso@math.unicaen.fr

Istituto Universitario di Architettura
Santa Croce, 191
30135 Venezia, Italy
zannier@brezza.iuav.unive.it