ACTA ARITHMETICA
135.4 (2008)

Small value estimates for the multiplicative group

by

Damien Roy (Ottawa)

1. Introduction. For applications to transcendental number theory, it would be desirable to extend the actual criteria for algebraic independence so that they deal more efficiently with polynomials taking small values on large subsets of a finitely generated subgroup of an algebraic group. At the moment, one could say that these criteria concentrate on the smallest non-zero value of each polynomial on such sets, regardless of the global distribution of values. A good illustration of the need for refined criteria, and our main motivation for this quest, is a conjectural small value estimate for the algebraic group $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}$ which is proposed in [6] and shown to be equivalent to Schanuel's conjecture. In a preceding paper [7], we explored the case of the additive group $\mathbb{G}_{\mathrm{a}}$. Here, we turn to the multiplicative group $\mathbb{G}_{\mathrm{m}}$. Although this is again an algebraic group of dimension one, we will see that it presents new challenges as roots of unity come into play.

Let $\mathbb{C}^\times$ denote the multiplicative group of non-zero complex numbers, let m be a positive integer, and let $\xi_1, \dots, \xi_m \in \mathbb{C}^\times$. An application of Dirichlet's box principle shows that, for any non-negative real numbers β, σ, τ, ν with

$$m\sigma + \tau < 1, \quad \beta > (m+1)\sigma + \tau, \quad \nu < 1 + \beta - m\sigma - \tau, \tag{1}$$

and for any positive integer n which is sufficiently large in terms of the preceding data, there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ of degree at most n and height at most $\exp(n^\beta)$ satisfying $|P^{[j]}(\xi_1^{i_1} \cdots \xi_m^{i_m})| < \exp(-n^\nu)$ for each choice of integers $i_1, \dots, i_m$ and j with $0 \le i_1, \dots, i_m \le n^\sigma$ and $0 \le j < n^\tau$. Here the *height* of P, denoted $H(P)$, is defined as the maximum of the absolute values of its coefficients divided by their greatest common divisor, and the expression $P^{[j]}$ stands for the jth divided derivative of P

2000 *Mathematics Subject Classification*: Primary 11J85; Secondary 11J81.

Key words and phrases: criterion for algebraic independence, simultaneous approximation, transcendence degree one, height and degree estimates.

Work partially supported by NSERC and CICMA.

(see §2). The goal of this paper is to establish the following partial converse to this statement.

THEOREM 1.1. *Let m be a positive integer, let $\xi_1, \dots, \xi_m$ be non-zero multiplicatively independent complex numbers which generate over $\mathbb{Q}$ a field of transcendence degree one, and let $\beta, \sigma, \tau, \nu \in \mathbb{R}$ with*

$$\sigma \geq 0, \quad \tau \geq 0, \quad \frac{5m+1}{m+5}\,\sigma + \tau < 1, \quad \beta \geq 1 + \sigma, \tag{2}$$

$$\nu > \begin{cases} 1 + \beta - \dfrac{3m-1}{m+5}\,\sigma - \tau & \text{if } m \geq 2, \\ 1 + \beta - \dfrac{5}{11}\,\sigma - \tau & \text{if } m = 1. \end{cases} \tag{3}$$

Then, for infinitely many positive integers n, there exists no non-zero polynomial $P \in \mathbb{Z}[T]$ with $\deg(P) \leq n$ and $H(P) \leq \exp(n^\beta)$ such that

$$\max\{|P^{[j]}(\xi_1^{i_1} \cdots \xi_m^{i_m})| \,; 0 \leq i_1, \dots, i_m \leq n^\sigma,\, 0 \leq j < n^\tau\} < e^{-n^\nu}. \tag{4}$$

When $m = 1$ and $\sigma = \tau = 0$, the above result reduces to the well-known Gel'fond transcendence criterion. So, for $m = 1$, it provides a gain of $(5/11)\sigma + \tau$ in the estimate for ν compared to Gel'fond's criterion. For $m \geq 2$, the gain is $((3m-1)/(m+5))\sigma + \tau$. On the other hand, the conditions (1) of application of Dirichlet's box principle put an upper bound on the gain that can be achieved. This suggests the possibility that Theorem 1.1 remains true for any integer $m \geq 1$ with the condition on ν relaxed to $\nu > 1 + \beta - m\sigma - \tau$, when $m\sigma + \tau < 1$, but we have not been able to prove this. Note that, when $\sigma = 0$, Theorem 1.1 deals with finitely many points and then it follows from Proposition 1 of [5]. The novelty here is that we deal with large numbers of points.

The proof of the above result is involved but the main underlying idea is simple and is inspired by techniques from zero estimates. If a polynomial $P \in \mathbb{Z}[T]$ takes small values at all points of the form ξ^a with ξ in a subset E of $\mathbb{C}^\times$ and a in a subset A of $\mathbb{N}^*$, then the polynomials $P(T^a)$ with $a \in A$ take small values at all points of E. Applying Corollary 3.2 of [7], one deduces that the product $\prod_{\xi \in E} |Q(\xi)|$ is small, where $Q(T)$ denotes the greatest common divisor in $\mathbb{Z}[T]$ of the polynomials $P(T^a)$ with $a \in A$. However, for this to be useful, we also need good upper bounds for the degree and height of $Q(T)$. The precise result that we use for this purpose is stated and proved in §7. For simplicity, we just mention here the following consequence of it, where $\mathbb{C}^\times_{\mathrm{tor}}$ stands for the group of roots of unity, the torsion part of $\mathbb{C}^\times$.

THEOREM 1.2. *Let $\beta, \delta, \mu \in \mathbb{R}$ with $0 < \delta$, $0 < \mu < 1$ and $1 + \mu < \beta$. Let n be a positive integer, let A be the set of all prime numbers p with $p \leq n^\mu$, let*

P be a non-zero polynomial of $\mathbb{Z}[T]$ of degree at most n and height at most $\exp(n^\beta)$ with no root in $\mathbb{C}^\times_{\mathrm{tor}} \cup \{0\}$, and let $Q \in \mathbb{Z}[T]$ be a greatest common divisor of the polynomials $P(T^a)$ with $a \in A$. If n is sufficiently large as a function of β, δ and μ, then $\deg(Q) \le n^{1-\mu+\delta}$ and $H(Q) \le \exp(n^{\beta-2\mu+\delta})$.

This result is the multiplicative analog of Theorem 1.2 of [7]. To achieve such non-trivial estimates on the degree and height of Q, the requirement that P has no root in $\mathbb{C}^\times_{\mathrm{tor}} \cup \{0\}$ is necessary. For example, if $P(T)$ is of the form $T^r(T^s-1)$ for some integers $r \ge 0$ and $s \ge 1$, then $P(T)$ divides $P(T^a)$ for any integer $a \ge 1$, and so $P(T)$ itself is the gcd of the latter collection of polynomials.

In practice, we start with a polynomial P satisfying (4) and we take for E a suitable subset of the subgroup of $\mathbb{C}^\times$ generated by $\xi_1, \dots, \xi_m$. In order to get appropriate degree and height estimates for the corresponding polynomial Q, we first need to remove from P a suitable cyclotomic factor. General estimates for this are given in §3. They require a lower bound for the absolute value of the cyclotomic factor on the set E. This is easy to achieve if one assumes that $\xi_1, \dots, \xi_m$ do not all have absolute value one, but the general case requires more elaborate arguments which occupy all of §4 and §5 for the case $m \ge 2$, and most of §9 in the case $m = 1$. The proof of Theorem 1.1 is completed in §8 for $m \ge 2$ and in §11 for $m = 1$. In both cases, we end up with a product $\prod_{\xi \in E} |Q(\xi)|$ being small and we need to choose $\xi \in E$ such that $|Q(\xi)|$ is small in order to be able to apply a standard transcendence criterion. The refined estimate that we obtain in the case $m = 1$ follows by observing that these values $|Q(\xi)|$ cannot be uniformly small. For this we use a combinatorial result proved in §10 as an extension of Proposition 9.1 of [7].

2. Notation and preliminaries. Throughout this paper, the symbols i, j, k are restricted to integers. We denote by $\mathbb{C}^\times$ the multiplicative group of non-zero complex numbers, by $\mathbb{C}^\times_{\mathrm{tor}}$ its torsion subgroup, by $\mathbb{N}$ the set of non-negative integers, and by $\mathbb{N}^*$ the set of positive integers. We also denote by $|E|$ the cardinality of an arbitrary set E, and by ϕ the Euler totient function. A *cyclotomic* polynomial is a monic polynomial of $\mathbb{Z}[T]$ whose roots lie in $\mathbb{C}^\times_{\mathrm{tor}}$. For any integer $j \ge 0$, we define the *jth divided derivative* of a polynomial $P \in \mathbb{C}[T]$ by $P^{[j]} = (j!)^{-1}P^{(j)}$ where $P^{(j)} = d^jP/dT^j$ is the usual jth derivative of P. Finally, the *length* $L(P)$ of a polynomial $P \in \mathbb{C}[T_1, \dots, T_m]$ is the sum of the absolute values of its coefficients.

Let K be a number field and let $d = [K : \mathbb{Q}]$. For each place v of K, we normalize the corresponding v-adic absolute value $|\ |_v$ of K so that it extends the usual absolute value of $\mathbb{Q}$ if v is Archimedean, or the usual p-adic absolute value of $\mathbb{Q}$ with $|p|_v = p^{-1}$ if v lies above a prime number p. We

also denote by K_v the completion of K at v, and by d_v its local degree. For any polynomial $P \in K_v[T_1, \dots, T_m]$, we define the v-adic norm $\|P\|_v$ of P as the largest v-adic absolute value of its coefficients. Finally, we define the *height* $H(P)$ of any polynomial $P \in K[T_1, \dots, T_m]$ by

$$H(P) = \prod_v \|P\|_v^{d_v/d}$$

where the product extends over all places v of K. This height is said to be *homogeneous* because it satisfies $H(aP) = H(P)$ for any non-zero element a of K, and *absolute* as it is independent of the choice of the number field K containing the coefficients of P. It therefore extends to a height on $\overline{\mathbb{Q}}[T_1, \dots, T_m]$ where $\overline{\mathbb{Q}}$ stands for the algebraic closure of $\mathbb{Q}$. In particular, the height of a non-zero polynomial $P \in \mathbb{Z}[T_1, \dots, T_m]$ is simply given by $H(P) = \|P\|/\mathrm{cont}(P)$ where $\|P\| = \|P\|_\infty$ is the maximum of the absolute values of its coefficients (we also use the latter notation for polynomials with complex coefficients), and where the *content* $\mathrm{cont}(P)$ of P is the gcd of its coefficients. We say that a non-zero polynomial of $\mathbb{Z}[T_1, \dots, T_m]$ is *primitive* if its content is 1, and that it is *primary* if it is a power of an irreducible element of $\mathbb{Z}[T_1, \dots, T_m]$. This implies that a non-constant primary polynomial of $\mathbb{Z}[T_1, \dots, T_m]$ is primitive.

In the present study, we frequently use the well-known fact that for one-variable polynomials $P_1, \dots, P_s \in \overline{\mathbb{Q}}[T]$ with product $P = P_1 \cdots P_s$, we have

$$e^{-\deg(P)} H(P) \le H(P_1) \cdots H(P_s) \le e^{\deg(P)} H(P). \tag{5}$$

For a single point $x \in \overline{\mathbb{Q}}$, we use the same notation $H(x)$ to denote the *inhomogeneous height* of x, that is, the height of the polynomial $T - x$. For $x \in K$, it is given by the formula $H(x) = \prod \max\{1, |x|_v\}^{d_v/d}$ where the product runs through all places v of K. As the field K can be chosen to be arbitrarily large, this shows that we have $H(x^m) = H(x)^{|m|}$ for any $m \in \mathbb{Z}$ and any non-zero $x \in \overline{\mathbb{Q}}$. From (5), we deduce that, if $x_1, \dots, x_s \in \overline{\mathbb{Q}}$ are all the roots of a non-zero polynomial $P \in \overline{\mathbb{Q}}[T]$ of degree s, listed with their multiplicities, then

$$e^{-s} H(P) \le H(x_1) \cdots H(x_s) \le e^s H(P). \tag{6}$$

The following lemma formalizes the standard procedure of "linearization" while handling multiplicities at the same time (cf. [7, Lemma 2.1]).

LEMMA 2.1. *Let $\varphi\colon \mathbb{Z}[T] \to [0, \infty)$ be a multiplicative function, let δ, d and Y be positive real numbers with $\delta < 1$ and $e^d \le Y$, and let $t \in \mathbb{N}^*$. Suppose that there exists a non-zero polynomial $Q_1 \in \mathbb{Z}[T]$ of degree at most d and height at most Y for which $Q = \gcd\{Q_1^{[j]}(T)\,; 0 \le j < t\}$ satisfies*

$\varphi(Q) \le \delta$. *Then there exists a primary polynomial* $S \in \mathbb{Z}[T]$ *with*

$$\deg(S) \le d/t, \quad H(S) \le Y^{2/t} \quad \text{and} \quad \varphi(S) \le \delta^{1/(6t)}.$$

By *multiplicative*, we mean that φ satisfies $\varphi(FG) = \varphi(F)\varphi(G)$ for any $F, G \in \mathbb{Z}[T]$. In our applications later, φ takes the form $\varphi(P) = \prod_{\xi \in E} |P(\xi)|$ for some fixed finite set E of complex numbers.

Proof. Let $Q = R_1 \cdots R_s$ be a factorization of Q into irreducible elements of $\mathbb{Z}[T]$. Since Q divides Q_1, we find

$$\prod_{i=1}^{s} (Y^{\deg(R_i)} H(R_i)^d) \le Y^{\deg(Q_1)} (e^{\deg(Q_1)} H(Q_1))^d \le Y^{3d}.$$

Therefore, upon writing $\delta = Y^{-3d\eta}$ for an appropriate value of $\eta > 0$, we obtain

$$\prod_{i=1}^{s} \varphi(R_i) = \varphi(Q) \le Y^{-3d\eta} \le \prod_{i=1}^{s} (Y^{\deg(R_i)} H(R_i)^d)^{-\eta}.$$

So, there is at least one index i with $1 \le i \le s$ such that the polynomial $R = R_i$ satisfies

$$\varphi(R) \le (Y^{\deg(R)} H(R)^d)^{-\eta}. \tag{7}$$

Since R divides $Q_1^{[j]}$ for $j = 0, \dots, t-1$, the polynomial Q_1 is divisible by R^t. This implies that $\deg(R) \le d/t$ and $H(R)^t \le e^d H(Q_1) \le Y^2$. Let $k \ge 1$ be the largest integer such that the polynomial $S = R^k$ satisfies $\deg(S) \le d/t$ and $H(S) \le Y^{2/t}$ (such an integer exists since $R \ne \pm 1$). We consider two cases. If $\deg(S) \ge d/(2t)$, then (7) leads to $\varphi(S) \le Y^{-\eta \deg(S)} \le Y^{-\eta d/(2t)} = \delta^{1/(6t)}$. On the other hand, if $\deg(S) < d/(2t)$, we have $\deg(R^{2k}) \le d/t$ and so $H(R^{2k}) \ge Y^{2/t}$. As $H(R^{2k}) \le e^{\deg(R^{2k})} H(R)^{2k} \le Y^{1/t} H(R)^{2k}$, we deduce that $H(R)^k \ge Y^{1/(2t)}$ and then (7) leads to $\varphi(S) \le H(R)^{-\eta k d} \le Y^{-\eta d/(2t)} = \delta^{1/(6t)}$, as in the previous case. ∎

For any finite subset E of $\mathbb{C}$ with at least two points, we define

$$\Delta_E = \prod_{\xi' \ne \xi} |\xi' - \xi|^{1/2} \tag{8}$$

where the product is taken over all ordered pairs (ξ, ξ') of distinct elements of E. When E consists of one point, we put $\Delta_E = 1$. The following result is a reformulation of Corollary 3.2 of [7] and our main tool to study families of polynomials taking small values on such a set E.

Proposition 2.2. *Let E be a non-empty finite set of complex numbers, let $n, t \in \mathbb{N}^*$ with $n \ge t|E|$, let $P_1, \dots, P_r \in \mathbb{Z}[T]$ be a finite sequence of $r \ge 2$ non-zero polynomials of degree at most n, and let $Q \in \mathbb{Z}[T]$ be their greatest*

common divisor. Then

$$\prod_{\xi\in E}\left(\frac{|Q(\xi)|}{\mathrm{cont}(Q)}\right)^t \le c_1(\max_{1\le i\le r} H(P_i))^{2n}\prod_{\xi\in E}(\max_{\substack{1\le i\le r\\ 0\le j<t}}|P_i^{[j]}(\xi)|)^t, \tag{9}$$

with $c_1 = e^{10n^2}(2+c_E)^{4nt|E|}\Delta_E^{-t^2}$, *where* $c_E = \max_{\xi\in E}|\xi|$ *and* Δ_E *is defined by* (8).

We conclude this section by stating the version of Gel'fond's criterion on which all our results ultimately rely. It is mainly due to Brownawell [1] and Waldschmidt [9] (see the comments after Lemma 2.2 of [7] for more details).

LEMMA 2.3. *Let* α, β *and* ε *be positive real numbers with* $\beta \ge \alpha$, *and let* $\xi_1,\dots,\xi_m$ *be a finite sequence of complex numbers which generate a field of transcendence degree one over* $\mathbb{Q}$. *For infinitely many integers* n, *there exists no polynomial* $P\in\mathbb{Z}[T_1,\dots,T_m]$ *of degree at most* n^α *and height at most* $\exp(n^\beta)$ *satisfying*

$$0 < |P(\xi_1,\dots,\xi_m)| \le \exp(-n^{\alpha+\beta+\varepsilon}).$$

3. The first step. The goal of this section is to establish the following result which represents the first step in the proof of our main theorem.

PROPOSITION 3.1. *Let* $M,n,t\in\mathbb{N}^*$ *and* $X\in\mathbb{R}$ *with* $1\le t\le n$. *Let* A *be a non-empty subset of* $\{1,\dots,M\}$, *and let* E *be a non-empty finite subset of* $\mathbb{C}^\times$ *with* $E\cap\mathbb{C}^\times_{\mathrm{tor}}=\emptyset$. *Finally, let* $P\in\mathbb{Z}[T]$ *be a non-zero polynomial with* $\deg(P)\le n$ *and* $H(P)\le X$, *written as a product* $P(T)=P_0(T)T^r\Phi(T)^t$ *where* $P_0\in\mathbb{Z}[T]$, $r\in\mathbb{N}$ *and* $\Phi\in\mathbb{Z}[T]$, *with* Φ *cyclotomic. Put*

$$\begin{aligned} c_E &= \max\{\max(|\xi|,|\xi|^{-1})\,;\xi\in E\},\\ \delta_\Phi &= \min\{|\Phi(\xi^a)|\,;a\in A,\,\xi\in E\},\\ \delta_P &= \max\{|P^{[j]}(\xi^a)|\,;a\in A,\,\xi\in E,\,0\le j<2t-1\},\end{aligned}$$

and assume that

$$t|E|\le Mn\le\frac{1}{10}\log X \quad\text{and}\quad (2+c_E)^{20t|E|}\le X. \tag{10}$$

Then the polynomial $Q(T)=\gcd\{P_0^{[j]}(T^a)\,;a\in A,\,0\le j<t\}$ (*computed in* $\mathbb{Z}[T]$) *satisfies*

$$\prod_{\xi\in E}\frac{|Q(\xi)|}{\mathrm{cont}(Q)}\le X^{5Mn/t}\Delta_E^{-t}\left(\frac{\delta_P}{\min(1,\delta_\Phi)^{3t}}\right)^{|E|}.$$

In practice, given P, we choose r to be the largest non-negative integer such that T^r divides $P(T)$, and $\Phi(T)$ to be the cyclotomic polynomial of $\mathbb{Z}[T]$ of largest degree such that $\Phi(T)^t$ divides $P(T)$. Then $Q(0)\ne 0$ and no

root of Q is a root of unity. As we saw in §1, such conditions are required in order to get good estimates on the degree and height of Q.

To prove the above result, we will apply Proposition 2.2 to the family of polynomials $P_0^{[j]}(T^a)$ with $a \in A$ and $0 \le j < t$. In order to estimate the absolute value of their derivatives at the elements of E, we first establish three lemmas.

LEMMA 3.2. *Let $\Phi \in \mathbb{C}[T]$, $t \in \mathbb{N}^*$ and $\xi \in \mathbb{C}$ with $\Phi(\xi) \neq 0$. For any integer $j \ge 0$, we have*

$$|(\Phi^{-t})^{[j]}(\xi)| \le \frac{1}{j!}\left((t+2j)\deg(\Phi)\|\Phi\|\max(1,|\xi|)^{\deg(\Phi)}\right)^j |\Phi(\xi)|^{-t-j}.$$

Proof. For each $j \ge 0$, the jth derivative of Φ^{-t} can be written in the form $(\Phi^{-t})^{(j)} = A_j\Phi^{-t-j}$ where A_j is a polynomial of $\mathbb{C}[T]$ satisfying $A_0 = 1$ and the recurrence relation $A_j = A'_{j-1}\Phi - (t+j-1)A_{j-1}\Phi'$ for $j \ge 1$. If $j \ge 1$, this gives $\deg(A_j) \le \deg(A_{j-1}) + \deg(\Phi)$ and by recurrence we get $\deg(A_j) \le j\deg(\Phi)$ for each $j \ge 0$. For the length of these polynomials, we also find, for $j \ge 1$,

$$\begin{aligned} L(A_j) &\le L(A'_{j-1})\|\Phi\| + (t+j-1)L(A_{j-1})\|\Phi'\| \\ &\le (\deg(A_{j-1}) + (t+j-1)\deg(\Phi))\|\Phi\|L(A_{j-1}) \\ &\le (t+2j-2)\deg(\Phi)\|\Phi\|L(A_{j-1}), \end{aligned}$$

which by recurrence gives $L(A_j) \le ((t+2j)\deg(\Phi)\|\Phi\|)^j$. The conclusion follows on using $|A_j(\xi)| \le L(A_j)\max(1,|\xi|)^{\deg(A_j)}$. ∎

LEMMA 3.3. *Let $n, t \in \mathbb{N}^*$ with $1 \le t \le n$, and let $P \in \mathbb{Z}[T]$ be a non-zero polynomial of degree at most n. Suppose that P factors as a product $P(T) = P_0(T)T^r\Phi(T)^t$, where $P_0 \in \mathbb{Z}[T]$, $r \in \mathbb{N}$ and $\Phi \in \mathbb{Z}[T]$, with Φ cyclotomic. Then, for each $\xi \in \mathbb{C}^\times$ with $\Phi(\xi) \neq 0$, we have*

$$\max_{0\le j<2t-1} |P_0^{[j]}(\xi)| \le \frac{e^{10n}\max(|\xi|,|\xi|^{-1})^{3n}}{\min(1,|\Phi(\xi)|)^{3t}} \max_{0\le j<2t-1} |P^{[j]}(\xi)|.$$

Proof. Since $P_0(T) = P(T)T^{-r}\Phi(T)^{-t}$, Leibniz' formula for the derivative of a product gives, for each integer $j \ge 0$,

$$P_0^{[j]}(T) = \sum_{j_0+j_1+j_2=j} P^{[j_0]}(T)\,(T^{-r})^{[j_1]}\,(\Phi(T)^{-t})^{[j_2]}, \tag{11}$$

where the summation runs through all decompositions of j as a sum of non-negative integers j_0, j_1, j_2. Let $\xi \in \mathbb{C}^\times$ with $\Phi(\xi) \neq 0$. As we have $r \le n$ and $t \le n$, we find, for each $j = 0, 1, \ldots, 2t$, that

$$|(T^{-r})^{[j]}(\xi)| = \binom{r+j-1}{j}|\xi|^{-r-j} \le \frac{(3n)^j}{j!}\max(1,|\xi|^{-1})^{3n}.$$

Since Φ^t divides P, we have $\deg(\Phi) \le n/t$, and since Φ is monic with all of its roots on the unit circle, we deduce that $\|\Phi\| \le 2^{\deg(\Phi)} \le 2^{n/t}$. Then, for $j = 0, 1, \dots, 2t$, Lemma 3.2 gives

$$|(\Phi^{-t})^{[j]}(\xi)| \le \frac{(5n)^j}{j!}\, 2^{2n} \max(1, |\xi|)^{2n} \min(1, |\Phi(\xi)|)^{-3t}.$$

Combining these estimates with (11), we conclude that

$$\max_{0\le j<2t-1} |P_0^{[j]}(\xi)| \le C \max(|\xi|, |\xi|^{-1})^{3n} \min(1, |\Phi(\xi)|)^{-3t} \max_{0\le j<2t-1} |P^{[j]}(\xi)|,$$

with

$$C = \sum_{j_1, j_2 \ge 0} \frac{(3n)^{j_1}(5n)^{j_2}}{j_1! j_2!}\, 2^{2n} \le e^{10n}. \ \blacksquare$$

LEMMA 3.4. *Let $a, t \in \mathbb{N}^*$, $P \in \mathbb{Z}[T]$ and $F(T) = P(T^a)$. For each $\xi \in \mathbb{C}$, we have*

$$\max_{0\le j<t} |F^{[j]}(\xi)| \le (2 + |\xi|)^{at} \max_{0\le j<t} |P^{[j]}(\xi^a)|.$$

Proof. Let $n = \deg(P)$. Expanding F and P in Taylor series around ξ and ξ^a respectively, we find

$$\sum_{j=0}^{an} F^{[j]}(\xi) T^j = F(T + \xi) = P((T + \xi)^a) = \sum_{j=0}^{n} P^{[j]}(\xi^a)((T + \xi)^a - \xi^a)^j.$$

Since T^t divides $((T + \xi)^a - \xi^a)^j$ for each $j \ge t$, this shows that the polynomials

$$\sum_{j=0}^{t-1} F^{[j]}(\xi) T^j \quad \text{and} \quad \sum_{j=0}^{t-1} P^{[j]}(\xi^a)((T + \xi)^a - \xi^a)^j$$

have the same coefficients of T^j for $j = 0, 1, \dots, t - 1$. Therefore the length of the first is bounded above by that of the second, and so we obtain

$$\sum_{j=0}^{t-1} |F^{[j]}(\xi)| \le \sum_{j=0}^{t-1} |P^{[j]}(\xi^a)|(1 + |\xi|)^{aj} \le (2 + |\xi|)^{at} \max_{0\le j<t} |P^{[j]}(\xi^a)|. \ \blacksquare$$

Proof of Proposition 3.1. Fix temporarily a choice of $a \in A$, $\xi \in E$ and $k \in \mathbb{N}$ with $k < t$, and put $\widetilde{P} = P_0^{[k]}(T^a)$. Since P_0 divides P and since $4n \le \log X$ by (10), we find

$$\deg(\widetilde{P}) \le a \deg(P_0) \le Mn, \qquad H(\widetilde{P}) \le 2^n H(P_0) \le 2^n e^n X \le X^{3/2}. \tag{12}$$

According to Lemma 3.4, we have

$$\begin{aligned} \max_{0\le j<t} |\widetilde{P}^{[j]}(\xi)| &\le (2 + |\xi|)^{at} \max_{0\le j<t} |P_0^{[k][j]}(\xi^a)| \\ &\le (2 + c_E)^{Mt} 2^{2t} \max_{0\le j<2t-1} |P_0^{[j]}(\xi^a)|. \end{aligned}$$

By Lemma 3.3, we also have

$$\max_{0\le j<2t-1}|P_0^{[j]}(\xi^a)| \le \frac{e^{10n}\max(|\xi^a|,|\xi^a|^{-1})^{3n}}{\min(1,|\Phi(\xi^a)|)^{3t}} \max_{0\le j<2t-1}|P^{[j]}(\xi^a)|$$
$$\le \frac{e^{10n}c_E^{3Mn}\delta_P}{\min(1,\delta_\Phi)^{3t}}.$$

Combining the last two estimates and using $t \le n \le Mn$ and $e \le 2 + c_E$, we obtain

$$\max_{0\le j<t}|\widetilde{P}^{[j]}(\xi)| \le \frac{(2+c_E)^{16Mn}\delta_P}{\min(1,\delta_\Phi)^{3t}}. \tag{13}$$

With the estimates (12) and (13) at hand, we are now ready to apply Proposition 2.2 to the collection of polynomials $P_0^{[k]}(T^a)$ with $a \in A$ and $0 \le k < t$. Using the hypotheses (10), this gives

$$\prod_{\xi\in E}\left(\frac{|Q(\xi)|}{\mathrm{cont}(Q)}\right)^t$$
$$\le e^{10(Mn)^2}(2+c_E)^{4(Mn)t|E|}\Delta_E^{-t^2}(X^{3/2})^{2Mn}\left(\frac{(2+c_E)^{16Mn}\delta_P}{\min(1,\delta_\Phi)^{3t}}\right)^{t|E|}$$
$$\le X^{5Mn}\Delta_E^{-t^2}\left(\frac{\delta_P}{\min(1,\delta_\Phi)^{3t}}\right)^{t|E|}. \ \blacksquare$$

4. Cyclotomic polynomials. In order to apply Proposition 3.1 to the proof of our main Theorem 1.1, we need a lower bound for the absolute value of a cyclotomic polynomial on an appropriate subset of a finitely generated subgroup of $\mathbb{C}^\times$. When the generators of that subgroup do not all have absolute value one, the required estimate is easy to derive. The reader who wants a proof of Theorem 1.1 under this simplifying assumption can skip this section and go directly to the last proposition of the next section where a suitable estimate is proved.

For the rest of this section, we fix a positive integer m and non-zero complex numbers $\xi_1, \dots, \xi_m$. For each m-tuple of integers $\mathbf{i} = (i_1, \dots, i_m)$, we write for shortness $\underline{\xi}^{\mathbf{i}} = \xi_1^{i_1} \cdots \xi_m^{i_m}$, and we define $\|\mathbf{i}\| = \max\{|i_1|, \dots, |i_m|\}$ to be the maximum norm of $\mathbf{i}$. Our goal is to prove the following result dealing with values of cyclotomic polynomials at the points $\underline{\xi}^{\mathbf{i}}$.

Proposition 4.1. *Let $d, N \in \mathbb{N}^*$ and $\delta \in \mathbb{R}$ with*

$$0 < \delta \le (8md^4N)^{-2md}, \tag{14}$$

and let $\Phi \in \mathbb{Z}[T]$ be a cyclotomic polynomial of degree $\le d$. Then there exist relatively prime positive integers $a_1, \dots, a_m, D$ with $D \le (2md^2N)^m$ such

that, upon defining

$$L(i_1, \dots, i_m) = a_1 i_1 + \cdots + a_m i_m$$

for each $(i_1, \dots, i_m) \in \mathbb{Z}^m$, *at least one of the following conditions holds*:

(1) *There exists a proper subspace* U *of* $\mathbb{Q}^m$ *such that* $|\Phi(\underline{\xi}^{\mathbf{i}})| \geq \delta$ *for any point* $\mathbf{i} \in \mathbb{Z}^m$ *with* $\mathbf{i} \notin U$, $\|\mathbf{i}\| \leq N$ *and* $\gcd(L(\mathbf{i}), D) = 1$.

(2) *There exists a root* Z *of* Φ *which is a root of unity of order exactly* D *such that, upon denoting by* G *the multiplicity of* Z *as a root of* Φ, *we have* $|\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}|^G \leq \delta^{1/2}$ *for each* $\mathbf{i} \in \mathbb{Z}^m$ *with* $\|\mathbf{i}\| \leq N$.

When condition (2) does not hold, condition (1) necessarily holds and provides the kind of estimate that we are looking for. This happens for example when $\xi_1, \dots, \xi_m$ do not all have absolute value one and when N is sufficiently large in terms of $\xi_1, \dots, \xi_m$, because under condition (2) we find, for each $j = 1, \dots, m$,

$$\big||\xi_j| - 1\big| \leq |\xi_j - Z^{a_j}| \leq \delta^{1/(2G)} \leq \delta^{1/(2d)} \leq (8md^4N)^{-m}.$$

In the next section we carry out an independent analysis of this situation (see Proposition 5.3). We also show that condition (2) cannot hold for N sufficiently large when $\xi_1, \dots, \xi_m$ are as in the statement of our main theorem, with $m \geq 2$.

Before going into the proof of Proposition 4.1, we also note that conditions (1) and (2) are almost mutually exclusive in the following sense. Suppose that condition (2) holds, and let $\mathbf{i}$ be any point of $\mathbb{Z}^m$ satisfying $\|\mathbf{i}\| \leq N$ and $\gcd(L(\mathbf{i}), D) = 1$. Then $|\underline{\xi}^{\mathbf{i}}| \leq 1 + \delta^{1/(2G)} \leq 2$, and $Z^{L(\mathbf{i})}$ is a conjugate of Z over $\mathbb{Q}$. So the latter is also a root of Φ of multiplicity G. Upon writing $\Phi(T) = \Psi(T)(T - Z^{L(\mathbf{i})})^G$ with $\Psi \in \mathbb{C}[T]$, we find that $|\Psi(\underline{\xi}^{\mathbf{i}})| \leq (|\underline{\xi}^{\mathbf{i}}| + 1)^d \leq 3^d$ (since Ψ is monic of degree at most d with all its roots of absolute value one), and thus $|\Phi(\underline{\xi}^{\mathbf{i}})| \leq 3^d \delta^{1/2}$.

The proof of Proposition 4.1 requires several lemmas about cyclotomic polynomials and their roots. The first three of them are quite general.

LEMMA 4.2. *Let* $d \in \mathbb{N}^*$, *let* $\Phi \in \mathbb{Z}[T]$ *be a cyclotomic polynomial of degree at most* d, *and let* ζ *be a root of* Φ. *Denote by* ℓ *the order of* ζ *as a root of unity, and by* g *its multiplicity as a root of* Φ. *Then*

$$\ell \leq \frac{2d \log_2(2d)}{g} \leq 2d^2, \tag{15}$$

where $\log_2$ *stands for the logarithm in base* 2.

Proof. The theory of cyclotomic fields gives $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(\ell)$ where ϕ denotes Euler's totient function. Since ζ is a root of Φ of multiplicity g, this implies that $g\phi(\ell) \leq d$. Putting $k = \omega(\ell) + 1$ where $\omega(\ell)$ denotes the number

of distinct prime factors of ℓ, we have $k \geq 1$,

$$\phi(\ell) = \ell \prod_{p|\ell} \left(1 - \frac{1}{p}\right) \geq \ell \prod_{i=2}^{k} \left(1 - \frac{1}{i}\right) = \frac{\ell}{k} \quad \text{and} \quad \ell \geq \prod_{p|\ell} p \geq k!.$$

Since $k! \geq k^2/2$, this gives $k \leq \sqrt{2\ell}$, so $\phi(\ell) \geq \sqrt{\ell/2}$, and thus we have $\ell \leq 2\phi(\ell)^2$. Since $k! \geq 2^{k-1}$, we also find $k \leq 1 + \log_2(\ell)$, which combined with the previous upper bound for ℓ gives $k \leq 2\log_2(2\phi(\ell))$. Since we also have $\phi(\ell) \leq d/g \leq d$, we conclude that $k \leq 2\log_2(2d)$ and consequently $\ell \leq k\phi(\ell) \leq 2(d/g)\log_2(2d)$. ∎

For roots of unity, Liouville's inequality takes a very simple form:

LEMMA 4.3. *Let ζ_1 and ζ_2 be two distinct roots of unity with respective orders ℓ_1 and ℓ_2. Then*

$$|\zeta_1 - \zeta_2| \geq \frac{4}{\ell_1 \ell_2}.$$

Proof. For $j = 1, 2$, write $\zeta_j = \exp(2\pi r_j \sqrt{-1})$ where r_j is a rational number with denominator ℓ_j. Upon subtracting from r_1 a suitable integer, we can arrange that $|r_1 - r_2| \leq 1/2$. Since $|\exp(t\sqrt{-1}) - 1| \geq 2|t|/\pi$ for any real number t with $|t| \leq \pi$, we deduce that

$$|\zeta_1 - \zeta_2| = |\exp(2\pi(r_1 - r_2)\sqrt{-1}) - 1| \geq 4|r_1 - r_2|.$$

Since $r_1 - r_2$ is a non-zero rational number with denominator dividing $\ell_1\ell_2$, we also have $|r_1 - r_2| \geq (\ell_1\ell_2)^{-1}$ and the conclusion follows. ∎

LEMMA 4.4. *Let $d \in \mathbb{N}^*$ and let $\Phi \in \mathbb{Z}[T]$ be a cyclotomic polynomial of degree at most d. Then, for any $\xi \in \mathbb{C}$, there exists a root ζ of Φ with*

$$|\xi - \zeta|^g \leq (2d^4)^d |\Phi(\xi)|, \tag{16}$$

where g denotes the multiplicity of ζ as a root of Φ.

Proof. Let ζ be a root of Φ which is closest to ξ, and let g be its multiplicity. Since Φ is monic, we can write $\Phi(T) = (T - \zeta_1) \cdots (T - \zeta_s)$ where $s \leq d$ is the degree of Φ and where $\zeta_1, \ldots, \zeta_s$ are roots of unity with $\zeta_1 = \cdots = \zeta_g = \zeta$. By Lemma 4.2, each ζ_j has order at most $2d^2$. Thus, for $j = g+1, \ldots, s$, Lemma 4.3 gives $|\zeta - \zeta_j| \geq d^{-4}$. For the same values of j we also have $|\zeta - \zeta_j| \leq |\xi - \zeta| + |\xi - \zeta_j| \leq 2|\xi - \zeta_j|$ by virtue of the choice of ζ, and so $|\xi - \zeta_j| \geq (2d^4)^{-1}$. This gives $|\Phi(\xi)| \geq |\xi - \zeta|^g (2d^4)^{g-s} \geq |\xi - \zeta|^g (2d^4)^{-d}$. ∎

The last lemma is more technical and provides the key to the proof of Proposition 4.1.

LEMMA 4.5. *Let $\ell, N \in \mathbb{N}^*$ and $\varrho \in \mathbb{R}$ with $0 < \varrho \leq (1/2)(mN)^{-m}$. Suppose that there exist linearly independent points $\mathbf{i}^{(1)}, \ldots, \mathbf{i}^{(m)}$ of $\mathbb{Z}^m$ of norm at most N, and roots of unity $\zeta_1, \ldots, \zeta_m$ of order at most ℓ such that $|\underline{\xi}^{\mathbf{i}^{(k)}} - \zeta_k| \leq \varrho$ for $k = 1, \ldots, m$. Then there exist a positive integer D with*

$D \le (\ell mN)^m$, a root of unity Z of order D, and non-zero integers $a_1, \dots, a_m$ with $\gcd(a_1, \dots, a_m, D) = 1$ such that, for each $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$ with norm $\|\mathbf{i}\| \le N$, we have

$$|\underline{\xi}^{\mathbf{i}} - Z^{a_1 i_1 + \cdots + a_m i_m}| \le 4(mN)^m \varrho. \tag{17}$$

Proof. For $k = 1, \dots, m$, we can write $\underline{\xi}^{\mathbf{i}^{(k)}} = \zeta_k(1 + \varrho_k)$ for a complex number ϱ_k with $|\varrho_k| \le \varrho$. Put $\varrho'_k = \log(1 + \varrho_k) = -\sum_{j=1}^{\infty}(-\varrho_k)^j/j$. Since $|\varrho_k| \le 1/2$, we find $|\varrho'_k| \le 2|\varrho_k|$, and so

$$\underline{\xi}^{\mathbf{i}^{(k)}} = \zeta_k \exp(\varrho'_k) \quad \text{with } |\varrho'_k| \le 2\varrho. \tag{18}$$

Let M be the square $m \times m$ matrix whose rows are $\mathbf{i}^{(1)}, \dots, \mathbf{i}^{(m)}$. For $j = 1, \dots, m$, let $(b_{j1}, \dots, b_{jm})$ denote the jth row of the adjoint of M, and let $\mathbf{e}_j$ denote the jth row of the $m \times m$ identity matrix. Since we have $\det(M)\mathbf{e}_j = b_{j1}\mathbf{i}^{(1)} + \cdots + b_{jm}\mathbf{i}^{(m)}$, we find by (18) that

$$\xi_j^{\det(M)} = \zeta_1^{b_{j1}} \cdots \zeta_m^{b_{jm}} \exp\Big(\sum_{k=1}^{m} b_{jk}\varrho'_k\Big). \tag{19}$$

Since $|b_{jk}| \le (m-1)!N^{m-1}$ for $k = 1, \dots, m$ and since $\det(M)$ is a non-zero integer, we deduce from (18) and (19) that

$$\xi_j = Z_j \exp(\varrho''_j) \quad \text{with } Z_j^{\det(M)} = \zeta_1^{b_{j1}} \cdots \zeta_m^{b_{jm}} \text{ and } |\varrho''_j| \le 2m!N^{m-1}\varrho. \tag{20}$$

Let Z be a generator of the subgroup of $\mathbb{C}_{\mathrm{tor}}^{\times}$ spanned by $Z_1, \dots, Z_m$, and let D be the order of Z. Since $Z^{\det(M)}$ belongs to the subgroup spanned by $\zeta_1, \dots, \zeta_m$ and since the latter have order at most ℓ, the order D of Z is at most $\ell^m|\det(M)| \le (\ell mN)^m$. For $j = 1, \dots, m$, we choose an integer $a_j \ge 1$ such that $Z_j = Z^{a_j}$. Then, because of the choice of Z, we have $\gcd(a_1, \dots, a_m, D) = 1$, and for each $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$ with $\|\mathbf{i}\| \le N$ we find by (20) that

$$\begin{aligned} &\underline{\xi}^{\mathbf{i}} = Z^{a_1 i_1 + \cdots + a_m i_m} \exp(\varrho'''_{\mathbf{i}}) \quad \text{with} \\ &|\varrho'''_{\mathbf{i}}| \le (mN)(2m!N^{m-1}\varrho) \le 2(mN)^m\varrho. \end{aligned} \tag{21}$$

Since $|\varrho'''_{\mathbf{i}}| \le 1$, we also have $|\exp(\varrho'''_{\mathbf{i}}) - 1| \le 2|\varrho'''_{\mathbf{i}}|$ and so (17) follows. ∎

Proof of Proposition 4.1. Let I_N denote the set of points $\mathbf{i} \in \mathbb{Z}^m$ with norm $\|\mathbf{i}\| \le N$, and let $I_{N,\Phi}$ denote the set of points $\mathbf{i} \in I_N$ such that $|\Phi(\underline{\xi}^{\mathbf{i}})| < \delta$. If $I_{N,\Phi}$ is contained in a proper subspace U of $\mathbb{Q}^m$, we are done. Assume the contrary. Then, since $I_{N,\Phi}$ is a finite set, there exists a smallest positive real number ϱ for which it contains m linearly independent points $\mathbf{i}^{(1)}, \dots, \mathbf{i}^{(m)}$ with the property that each of the complex numbers $\underline{\xi}^{\mathbf{i}^{(1)}}, \dots, \underline{\xi}^{\mathbf{i}^{(m)}}$ is at a distance $\le \varrho$ from a zero of Φ. Lemma 4.4 shows that,

for each $\mathbf{i} \in I_{N,\Phi}$, there exists a root ζ of Φ with

$$|\underline{\xi}^{\mathbf{i}} - \zeta|^g \le (2d^4)^d \delta, \tag{22}$$

where g denotes the multiplicity of ζ. Since $g \le d$, this implies that $\varrho \le 2d^4\delta^{1/d}$. Since the hypothesis (14) gives $2d^4\delta^{1/d} \le (2mN)^{-m}$ and since, by Lemma 4.2, any root ζ of Φ has order $\le 2d^2$, Lemma 4.5 provides us with relatively prime positive integers $a_1, \dots, a_m, D$ with $D \le (2d^2mN)^m$, and a root of unity Z of order D, such that for each $\mathbf{i} = (i_1, \dots, i_m) \in I_N$, we have

$$|\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}| \le 4(mN)^m \varrho, \quad \text{where} \quad L(\mathbf{i}) = a_1 i_1 + \cdots + a_m i_m. \tag{23}$$

If we choose $\mathbf{i} \in I_{N,\Phi}$ and if ζ is a root of Φ satisfying (22), this gives

$$|\zeta - Z^{L(\mathbf{i})}| \le (1 + 4(mN)^m) 2d^4 \delta^{1/d}. \tag{24}$$

As ζ and $Z^{L(\mathbf{i})}$ are roots of unity of order at most $2d^2$ and D respectively, and since by (14) the right hand side of (24) is bounded above by $4d^4(4mN)^m(8md^4N)^{-2m} < 4D^{-1}(2d^2)^{-1}$, we conclude, by Lemma 4.3, that both roots of unity are equal. Therefore, $Z^{L(\mathbf{i})} = \zeta$ is a root of Φ when $\mathbf{i} \in I_{N,\Phi}$.

Finally, let $I_{N,\Phi,D}$ denote the set of points $\mathbf{i} \in I_{N,\Phi}$ with $\gcd(L(\mathbf{i}), D) = 1$. Again, if this set is contained in a proper subspace of $\mathbb{Q}^m$, the first condition of the proposition holds. Suppose on the contrary that $I_{N,\Phi,D}$ contains m linearly independent points. For each $\mathbf{i} \in I_{N,\Phi,D}$, the root of unity $Z^{L(\mathbf{i})}$ is a conjugate of Z over $\mathbb{Q}$, so it is a root of Φ of the same multiplicity G as Z, and the inequality (22) gives $|\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}|^G \le (2d^4)^d\delta$. As $I_{N,\Phi,D}$ contains m linearly independent points, this means that $\varrho^G \le (2d^4)^d\delta$. By (23) and the fact that $G \le d$, we conclude that, for each $\mathbf{i} \in I_N$, we have

$$|\underline{\xi}^{\mathbf{i}} - Z^{L(\mathbf{i})}|^G \le (4(mN)^m\varrho)^G \le (4mN)^{md}(2d^4)^d\delta \le \delta^{1/2}. \ \blacksquare$$

5. Avoiding cyclotomic factors in rank at least two. In this section, we consider two instances where only the first alternative in Proposition 4.1 holds. As observed in the preceding section, the simplest case is when $\xi_1, \dots, \xi_m$ do not all have absolute value one. The reader who wants to restrict to this situation can go directly to Proposition 5.3, where a short independent proof is given, and omit the rest of the section. The second case is when $\xi_1, \dots, \xi_m$ are multiplicatively independent with $m \ge 2$, and generate over $\mathbb{Q}$ a field of transcendence degree one. To show that the latter condition is sufficient, we first establish the following measure of simultaneous approximation by roots of unity, where ϕ stands for the Euler totient function.

PROPOSITION 5.1. *Let $m \ge 2$ be an integer, and let $\xi_1, \dots, \xi_m \in \mathbb{C}^\times$ be multiplicatively independent non-zero complex numbers which generate over $\mathbb{Q}$ a field of transcendence degree one. Then, for any choice of positive*

integers $a_1, \dots, a_m, D$ and for any root of unity $Z \in \mathbb{C}^\times_{\mathrm{tor}}$ of order D, we have

$$\max_{1\le j\le m} |\xi_j - Z^{a_j}| > c^{\phi(D)} \tag{25}$$

where c is a constant depending only on $\xi_1, \dots, \xi_m$ with $0 < c \le 1$.

In the proof below as well as in the rest of the section, we use the same notation as in Section 4. Namely, we denote by $\|\mathbf{i}\|$ the maximum norm of an integer point $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$, and we define $\underline{\xi}^{\mathbf{i}} = \xi_1^{i_1} \cdots \xi_m^{i_m}$.

Proof. The field $R = \mathbb{Q}(\xi_1, \dots, \xi_m)$ is a field of functions in one variable over $\mathbb{Q}$ (see Chapter 1 of [2]). Let K denote its field of constants and, for $j = 1, \dots, m$, let $\mathfrak{b}_j$ denote the divisor of poles of ξ_j. Let J be the ideal of polynomials of $\mathbb{Q}[T_1, \dots, T_m]$ which vanish at the point $(\xi_1, \dots, \xi_m)$, and let $P_1, \dots, P_s$ be a system of generators of this ideal, chosen in $\mathbb{Z}[T_1, \dots, T_m]$. Define

$$c_1 = \max_{1\le k\le s} (L(P_k) \max_{1\le j\le m} (1 + |\xi_j|)^{\deg(P_k)}), \qquad c_2 = [K : \mathbb{Q}] \sum_{j=1}^{m} \deg(\mathfrak{b}_j),$$

and choose a real number c with $0 < c < c_1^{-1}$ such that (25) holds whenever $D \le (3c_2)^6$ (this involves a finite number of inequalities). We claim that, for such a value of c, the estimate (25) holds in general.

To prove this, suppose on the contrary that there exist positive integers $a_1, \dots, a_m, D$ and a root of unity Z of order D which satisfy

$$\max_{1\le j\le m} |\xi_j - Z^{a_j}| \le c^{\phi(D)}.$$

Upon replacing $a_1, \dots, a_m$, D and Z respectively by $a_1/a, \dots, a_m/a$, D/a and Z^a where $a = \gcd(a_1, \dots, a_m, D)$, we may assume without loss of generality that $a_1, \dots, a_m, D$ are relatively prime. For each $k = 1, \dots, s$, the norm of $P_k(Z^{a_1}, \dots, Z^{a_m})$ from $\mathbb{Q}(Z)$ to $\mathbb{Q}$ is an integer given by

$$\mathrm{N}_{\mathbb{Q}(Z)/\mathbb{Q}}(P_k(Z^{a_1}, \dots, Z^{a_m})) = \prod_{\substack{1\le j\le D\\ \gcd(j,D)=1}} P_k(Z^{ja_1}, \dots, Z^{ja_m}).$$

Since $|P_k(Z^{a_1}, \dots, Z^{a_m})| = |P_k(\xi_1, \dots, \xi_m) - P_k(Z^{a_1}, \dots, Z^{a_m})|$ is bounded above by $c_1 \max_{1\le j\le m} |\xi_j - Z^{a_j}|$, and since $|P_k(Z^{ja_1}, \dots, Z^{ja_m})| \le L(P_k) \le c_1$ for each integer j, we deduce that

$$|\mathrm{N}_{\mathbb{Q}(Z)/\mathbb{Q}}(P_k(Z^{a_1}, \dots, Z^{a_m}))| \le c_1^{\phi(D)} \max_{1\le j\le m} |\xi_j - Z^{a_j}| \le (c_1 c)^{\phi(D)} < 1.$$

Thus the norm of $P_k(Z^{a_1}, \dots, Z^{a_m})$ is 0 and so we have $P_k(Z^{a_1}, \dots, Z^{a_m}) = 0$ for $k = 1, \dots, s$. According to [2, Ch. 1, §4, Cor. 1], this implies the existence of a place $\mathfrak{p}$ of R which is a common zero of $\xi_1 - Z^{a_1}, \dots, \xi_m - Z^{a_m}$.

The residue field of this place contains $\mathbb{Q}[Z^{a_1}, \dots, Z^{a_m}]$, which is simply $\mathbb{Q}(Z)$ since $\gcd(a_1, \dots, a_m, D) = 1$. Thus, we have

$$[K : \mathbb{Q}] \deg(\mathfrak{p}) \geq [\mathbb{Q}(Z) : \mathbb{Q}] = \phi(D). \tag{26}$$

Define $L(\mathbf{i}) = a_1 i_1 + \cdots + a_m i_m$ for each $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m$, and choose any non-zero point $\mathbf{i} \in \mathbb{Z}^m$ such that $L(\mathbf{i}) \equiv 0 \bmod D$. Since $\xi_1, \dots, \xi_m$ are multiplicatively independent, the difference $\eta = \underline{\xi}^{\mathbf{i}} - 1$ is a non-zero element of R. Let $\mathfrak{a}$ denote its divisor of zeros, and $\mathfrak{b}$ its divisor of poles. Then $\mathfrak{a}$ and $\mathfrak{b}$ have the same degree. Similarly, for each $j = 1, \dots, m$ the divisor of zeros $\mathfrak{a}_j$ of ξ_j has the same degree as its divisor of poles $\mathfrak{b}_j$. Since $\mathfrak{b}$ is also the divisor of poles of $\underline{\xi}^{\mathbf{i}} = \xi_1^{i_1} \cdots \xi_m^{i_m}$, we deduce that

$$\deg(\mathfrak{b}) \leq \|\mathbf{i}\| \sum_{j=1}^{m} \deg(\mathfrak{b}_j).$$

On the other hand, since $Z^{L(\mathbf{i})} = 1$, the place $\mathfrak{p}$ is a zero of η and so we have $\deg(\mathfrak{a}) \geq \deg(\mathfrak{p})$. Combining this with (26) and the above inequality, we conclude that

$$\phi(D) \leq [K : \mathbb{Q}] \deg(\mathfrak{p}) \leq [K : \mathbb{Q}] \deg(\mathfrak{a}) = [K : \mathbb{Q}] \deg(\mathfrak{b}) \leq c_2 \|\mathbf{i}\|.$$

This observation implies that the function $f \colon \mathbb{Z}^m \to \mathbb{Z}/D\mathbb{Z}$ defined by $f(\mathbf{i}) = L(\mathbf{i}) + D\mathbb{Z}$ ($\mathbf{i} \in \mathbb{Z}^m$) is injective on the set of points $\mathbf{i} \in \mathbb{N}^m$ with $\|\mathbf{i}\| < c_2^{-1}\phi(D)$, and therefore we have

$$D \geq (c_2^{-1}\phi(D))^m \geq (c_2^{-1}\phi(D))^2. \tag{27}$$

On the other hand, since Z is a root of a cyclotomic polynomial of degree $\phi(D)$, Lemma 4.2 gives $D \leq 2\phi(D)\log_2(2\phi(D)) \leq 3\phi(D)\log(2\phi(D))$. Since $\log(x) \leq \sqrt{x}$ for any positive real number x, this leads to $D \leq (3\phi(D))^{3/2}$, which combined with (27) gives $D \leq (3c_2)^6$. This is a contradiction since we chose c so that (25) holds for such a value of D. ∎

Combining the above result with Proposition 4.1, we obtain:

COROLLARY 5.2. *Let m, $\xi_1, \dots, \xi_m$ and c be as in the statement of Proposition* 5.1. *Let $d, N \in \mathbb{N}^*$ and $\delta \in \mathbb{R}$ with*

$$0 < \delta \leq \min\{(8md^4N)^{-m}, c\}^{2d}, \tag{28}$$

and let $\Phi \in \mathbb{Z}[T]$ be a cyclotomic polynomial of degree $\leq d$. Then there exist relatively prime positive integers $a_1, \dots, a_m, D$ with $D \leq (2md^2N)^m$ and a proper subspace U of $\mathbb{Q}^m$ such that $|\Phi(\underline{\xi}^{\mathbf{i}})| \geq \delta$ for any point $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m \setminus U$ with $\|\mathbf{i}\| \leq N$ and $\gcd(a_1 i_1 + \cdots + a_m i_m, D) = 1$.

Proof. Let Z be a root of Φ, let D denote its order as a root of unity, and let G denote its multiplicity as a root of Φ. Since $d \geq \deg(\Phi) \geq G\phi(D)$,

Proposition 5.1 gives

$$\max_{1\le j\le m} |\xi_j - Z^{a_j}|^G > c^{G\phi(D)} \ge c^d \ge \delta^{1/2}$$

for any choice of positive integers $a_1, \dots, a_m$. The conclusion follows by Proposition 4.1. ∎

The next result provides a substitute for Corollary 5.2 when $\xi_1, \dots, \xi_m$ do not all have absolute value one.

PROPOSITION 5.3. *Let $m \ge 2$ be an integer, let $\xi_1, \dots, \xi_m \in \mathbb{C}^\times$ be non-zero complex numbers not all of absolute value* 1, *and let N be a positive integer. If N is sufficiently large, there exists a proper subspace U of $\mathbb{Q}^m$ such that $|\Phi(\underline{\xi}^{\mathbf{i}})| \ge (8mN)^{-md}$ for each positive integer d, each cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ of degree $\le d$, and each point $\mathbf{i} \in \mathbb{Z}^m \setminus U$ with $\|\mathbf{i}\| \le N$.*

Proof. Write $\xi_j = \exp(u_j + v_j\sqrt{-1})$ with $u_j, v_j \in \mathbb{R}$ for $j = 1, \dots, m$. Then $u_1, \dots, u_m$ are not all zero, and by a result of Dirichlet (see for example [8, Ch. II, Thm. 1A]), there exist integers $a_1, \dots, a_m$ and b satisfying the conditions $1 \le b \le (2mN)^m$ and $|bu_j - a_j| \le (2mN)^{-1}$ for $j = 1, \dots, m$. If N is large enough, the integers $a_1, \dots, a_m$ are not all zero, and so the equation $a_1x_1 + \cdots + a_mx_m = 0$ defines a proper subspace U of $\mathbb{Q}^m$. For any $\mathbf{i} = (i_1, \dots, i_m) \in \mathbb{Z}^m \setminus U$ with $\|\mathbf{i}\| \le N$, we have $|a_1i_1 + \cdots + a_mi_m| \ge 1$ and thus

$$\begin{aligned} |u_1i_1 + \cdots + u_mi_m| &\ge \frac{1}{b}\Big|\sum_{j=1}^m a_ji_j\Big| - \frac{1}{b}\sum_{j=1}^m |bu_j - a_j|\,|i_j| \\ &\ge \frac{1}{b} - \frac{1}{b}\, m(2mN)^{-1}N = \frac{1}{2b} \ge (4mN)^{-m}. \end{aligned}$$

Since $|\exp(x) - 1| \ge |x|/2$ for each $x \in \mathbb{R}$ with $|x| \le 1/2$, we deduce that for the same choice of $\mathbf{i}$ and any root of unity $\zeta \in \mathbb{C}^\times_{\mathrm{tor}}$, we have

$$\begin{aligned} |\underline{\xi}^{\mathbf{i}} - \zeta| &\ge \big||\underline{\xi}^{\mathbf{i}}| - 1\big| = |\exp(u_1i_1 + \cdots + u_mi_m) - 1| \\ &\ge 1 - \exp(-(4mN)^{-m}) \ge (8mN)^{-m}. \end{aligned}$$

Consequently, for any positive integer d and any cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ of degree $\le d$, we get $|\Phi(\underline{\xi}^{\mathbf{i}})| \ge (8mN)^{-md}$. ∎

6. Estimates for an intersection. Throughout this section, we fix an abelian group $\mathbb{G}$ with its group law written multiplicatively, and we fix a finite set of prime numbers A with cardinality at least 2. We denote by $\mathbb{G}_{\mathrm{tor}}$ the torsion subgroup of $\mathbb{G}$. For each subset E of $\mathbb{G}$, we define

$$\mathcal{O}(E) = \{x^p\,;\, x \in E,\ p \in A\}.$$

For a singleton $\{x\}$, we simply write $\mathcal{O}(x)$ to denote $\mathcal{O}(\{x\})$. Then, for any subset E of $\mathbb{G}$, we have $\mathcal{O}(E) = \bigcup_{x\in E} \mathcal{O}(x)$. For each $x \in \mathbb{G}$ and each integer

$k \geq 1$, we also define $C_k(x)$ to be the set of all elements y of $\mathbb{G}$ which satisfy a relation of the form

$$x^{p_1 \cdots p_k} = y^{q_1 \cdots q_k} \tag{29}$$

for a choice of prime numbers $p_1, \ldots, p_k, q_1, \ldots, q_k$ in A (not necessarily distinct). We also define $C_0(x) = \{x\}$. With this notation, the main result of this section reads as follows:

PROPOSITION 6.1. *Let E and F be finite non-empty subsets of $\mathbb{G}$ with $\mathcal{O}(E) \subseteq F$ and $E \cap \mathbb{G}_{\mathrm{tor}} = \emptyset$. Suppose that*

$$|F| \leq \frac{1}{2^{l+1}(l+1)!} \binom{|A|}{l+2} \tag{30}$$

for some integer l with $0 \leq l \leq |A| - 2$. Then, there exist an integer $r \geq 1$, a sequence of points $x_1, \ldots, x_r$ of E, and partitions $E = E_1 \amalg \cdots \amalg E_r$ and $F = F_1 \amalg \cdots \amalg F_r \amalg F_{r+1}$ of E and F which, for $i = 1, \ldots, r$, satisfy

$$\text{(a) } E_i \subseteq C_l(x_i), \quad \text{(b) } F_i \subseteq \mathcal{O}(E_i), \quad \text{(c) } |F_i| \geq \frac{|A| - l}{2(l+1)} |E_i|.$$

This result can be viewed as a generalization of Proposition 6.2 of [7] (see the remark at the end of this section for more details on how to derive the latter from the former). Its proof will follow the same general pattern, although additional difficulties come into play due to the fact that $\mathbb{G}$ may contain non-trivial torsion elements. To deal with these, we use several additional notions.

First of all, we say that two elements x and y of $\mathbb{G}$ are *A-equivalent* and we write $x \sim_A y$ if there exist finite sequences $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_l)$ of elements of A such that

$$x^{p_1 \cdots p_k} = y^{q_1 \cdots q_l}. \tag{31}$$

This defines an equivalence relation on $\mathbb{G}$. In view of the preceding definitions, for any $x \in \mathbb{G}$ and any integer $k \geq 0$, the equivalence class of x contains $C_k(x)$.

Fix a non-torsion element x of $\mathbb{G}$ and a point y in the same equivalence class. Then y is also a non-torsion element of G. Moreover, if $\langle x \rangle$ denotes the subgroup of $\mathbb{G}$ generated by x, then the set of integers i such that $y^i \in \langle x \rangle$ is a non-trivial subgroup of $\mathbb{Z}$. We define $\mathrm{den}_x(y)$ to be the positive generator n of this group. Then, since x is non-torsion, there exists a unique integer m such that $y^n = x^m$, and we define $\mathrm{num}_x(y) = m$. Note that these integers m and n may not be relatively prime, and therefore the fraction m/n may not be in reduced form. However, the following lemma shows useful properties for these notions of logarithmic "numerator" and "denominator" of y with respect to x.

LEMMA 6.2. *Let x and y be non-torsion elements of $\mathbb{G}$ in the same equivalence class. Put $n = \mathrm{den}_x(y)$ and $m = \mathrm{num}_x(y)$, and choose elements $p_1, \dots, p_k, q_1, \dots, q_l$ of A such that (31) holds. Then m (resp. n) is a positive divisor of $p_1 \cdots p_k$ (resp. $q_1 \cdots q_l$), and we have*

$$\frac{m}{n} = \frac{p_1 \cdots p_k}{q_1 \cdots q_l}. \tag{32}$$

Moreover, if q is an element of A not dividing n, then the point $z = y^q$ satisfies $\mathrm{den}_x(z) = n$ and $\mathrm{num}_x(z) = qm$.

Proof. Since $x \notin \mathbb{G}_{\mathrm{tor}}$, the equality (31) combined with $y^n = x^m$ leads to (32). Moreover, as (31) gives $y^{q_1 \cdots q_l} \in \langle x \rangle$, it follows from the definition of $\mathrm{den}_x(y)$ that n is a positive divisor of $q_1 \cdots q_l$. Then, since all the elements of A are positive, we deduce from (32) that m is a positive divisor of $p_1 \cdots p_k$. This proves the first part of the lemma.

For the second part, fix a prime number $q \in A$ not dividing n. Put $z = y^q$, $n' = \mathrm{den}_x(z)$ and $m' = \mathrm{num}_x(z)$. Since $z^n = y^{qn} = x^{qm} \in \langle x \rangle$, it follows, by definition of n', that n' divides n. Moreover, since $y^{qn'} = z^{n'} = x^{m'} \in \langle x \rangle$, it also follows from the definition of n that n divides qn'. Since, by hypothesis, q and n are relatively prime, and since n and n' are positive, these two divisibility relations imply that $n = n'$. Then, since $x \notin \mathbb{G}_{\mathrm{tor}}$, the equality $x^{m'} = z^n = x^{qm}$ implies that $m' = qm$. ∎

For any integer $k \geq 0$, any non-torsion point x of $\mathbb{G}$ and any subset E of $\mathbb{G}$, we define

$$C_k(x, E) = C_k(x) \cap E \quad \text{and} \quad D_k(x, E) = \mathcal{O}(C_k(x, E)).$$

With this notation, the first part of Lemma 6.2 shows that, for each $y \in C_k(x, E)$ and each $z \in D_k(x, E)$, the integers $\mathrm{den}_x(y)$, $\mathrm{num}_x(y)$ and $\mathrm{den}_x(z)$ are products of at most k elements of A, while $\mathrm{num}_x(z)$ is a product of at most $k + 1$ elements of A, counting multiplicities. We also note that if a subset F of $\mathbb{G}$ contains $\mathcal{O}(E)$, then it contains $D_k(x, E)$. The next lemma compares the sizes of $C_k(x, E)$ and $D_k(x, E)$.

LEMMA 6.3. *Let E be a finite subset of $\mathbb{G}$, let $k \geq 0$ be an integer, and let $x \in \mathbb{G}$ with $x \notin \mathbb{G}_{\mathrm{tor}}$. Then*

$$|D_k(x, E)| \geq \frac{|A| - k}{k + 1} |C_k(x, E)|.$$

Proof. Put $C = C_k(x, E)$ and $D = \mathcal{O}(C)$, so that $D = D_k(x, E)$. We denote by N the set of all pairs $(y, q) \in C \times A$ such that q divides $\mathrm{den}_x(y)$, and we put $P = (C \times A) \setminus N$. Then, since N and P form a partition of $C \times A$, we have

$$|N| + |P| = |C|\,|A|. \tag{33}$$

For any given $y \in C$, the integer $\mathrm{den}_x(y)$ is a product of at most k prime numbers (including multiplicities). Therefore there are at most k distinct elements q of A such that $(y,q) \in N$. This being true for each $y \in C$, we deduce that

$$|N| \le k|C|. \tag{34}$$

Consider the surjective map $\varphi\colon C \times A \to D$ given by $\varphi(y,q) = y^q$ for each $(y,q) \in C \times A$. We claim that, for each $z \in D$, we have $|\varphi^{-1}(z) \cap P| \le k+1$. If we admit this result, then we find

$$|P| = |\varphi^{-1}(D) \cap P| \le (k+1)|D|,$$

and by combining this estimate with (33) and (34), we deduce that

$$(k+1)|D| \ge |P| = |A|\,|C| - |N| \ge (|A| - k)|C|,$$

as announced.

To prove the above claim, suppose that $(y,q) \in \varphi^{-1}(z) \cap P$ for some fixed $z \in D$. Put $n = \mathrm{den}_x(y)$ and $m = \mathrm{num}_x(y)$. By hypothesis, we have $y^q = z$ and q is prime to n. According to Lemma 6.2, this implies that $\mathrm{den}_x(z) = n$ and $\mathrm{num}_x(z) = qm$. So, n is known (it depends only on x and z) and q is a prime divisor of $\mathrm{num}_x(z)$. Moreover, since $z \in D$, the integer $\mathrm{num}_x(z)$ is a product of at most $k+1$ prime numbers of A. So, this leaves at most $k+1$ possibilities for q. Once q is known, the relation $\mathrm{num}_x(z) = qm$ uniquely determines m, and the conditions $y^q = z$ and $y^n = x^m$ in turn determine y: since q is prime to n, we can write $1 = aq + bn$ with $a, b \in \mathbb{Z}$ and then we find $y = z^a x^{bm}$. Thus $\varphi^{-1}(z)$ contains at most $k+1$ elements (y,q) of P. ∎

Lemma 6.4. *Let E be a finite subset of $\mathbb{G}$, let $k \ge 0$ be an integer, and let $x \in \mathbb{G}$ with $x \notin \mathbb{G}_{\mathrm{tor}}$. Then*

$$|D_k(x,E) \cap \mathcal{O}(E \setminus C_k(x,E))| \le (k+1)|C_{k+1}(x,E)|.$$

Proof. It suffices to show that, for any $y \in E \setminus C_k(x,E)$ such that $D_k(x,E)$ meets $\mathcal{O}(y)$, we have $y \in C_{k+1}(x,E)$ and $|D_k(x,E) \cap \mathcal{O}(y)| \le k+1$. Fix such a choice of y (assuming that there is one). Since $D_k(x,E) \cap \mathcal{O}(y) \ne \emptyset$, there exist $p, q \in A$ and $z \in C_k(x,E)$ such that $y^q = z^p$. Moreover, since $z \in C_k(x,E)$, there also exist $p_1, \dots, p_k, q_1, \dots, q_k \in A$ such that $z^{q_1 \cdots q_k} = x^{p_1 \cdots p_k}$. Combining these two relations, we obtain

$$y^{qq_1 \cdots q_k} = x^{pp_1 \cdots p_k}, \tag{35}$$

which shows that $y \in C_{k+1}(x,E)$. Put $n = \mathrm{den}_x(y)$ and $m = \mathrm{num}_x(y)$. By Lemma 6.2, the equality (35) also implies that n divides $qq_1 \cdots q_k$ and that $m/n = (pp_1 \cdots p_k)/(qq_1 \cdots q_k)$. In particular, the factorizations of m and n into prime numbers have the same length: they involve the same number of elements of A, counting multiplicities. If j is this length, then the equality $y^n = x^m$ means that $y \in C_j(x,E)$. Since $y \notin C_k(x,E)$, we must have $j > k$.

It follows that $j = k+1$ and $n = qq_1 \cdots q_k$. In particular, q is one of the prime factors of n. Since $n = \mathrm{den}_x(y)$ has at most $k+1$ distinct prime factors, we conclude that $|D_k(x,E) \cap \mathcal{O}(y)| \le k+1$. ∎

Proof of Proposition 6.1. We proceed by induction on $|E|$. Fix a choice of $x \in E$. We claim that there exists an index k with $0 \le k \le l$ such that the sets $C_k = C_k(x,E)$ and $D_k = D_k(x,E)$ satisfy

$$|D_k \setminus \mathcal{O}(E \setminus C_k)| \ge \frac{|A|-k}{2(k+1)}\,|C_k|. \tag{36}$$

If we admit this statement then, for such k, the sets $E_1 = C_k$ and $F_1 = D_k \setminus \mathcal{O}(E \setminus C_k)$ satisfy conditions (a)–(c) of Proposition 6.1 for $i = 1$ and the choice of $x_1 = x$. Put $E' = E \setminus E_1$ and $F' = F \setminus F_1$. Then we have $E = E_1 \amalg E'$, $F = F_1 \amalg F'$ and $\mathcal{O}(E') \subseteq F'$. If $E' = \emptyset$, this proves the proposition with $r = 1$ and $F_2 = F'$. Otherwise, we may assume, by induction, that the proposition applies to E' and F', and the conclusion follows.

To prove the above claim, suppose on the contrary that (36) does not hold for $k = 0, 1, \ldots, l$. Then

$$|D_k| < |D_k \cap \mathcal{O}(E \setminus C_k)| + \frac{|A|-k}{2(k+1)}\,|C_k| \quad (0 \le k \le l).$$

Combining this with the lower bound for $|D_k|$ provided by Lemma 6.3 and the upper bound for $|D_k \cap \mathcal{O}(E \setminus C_k)|$ provided by Lemma 6.4, we obtain

$$\frac{|A|-k}{2(k+1)^2}\,|C_k| < |C_{k+1}| \quad (0 \le k \le l).$$

Since $C_0 = \{x\}$ has cardinality 1, these inequalities lead to $|C_{l+1}(x,E)| > (2^{l+1}(l+1)!)^{-1}\binom{|A|}{l+1}$, so by Lemma 6.3, $|D_{l+1}(x,E)| > (2^{l+1}(l+1)!)^{-1}\binom{|A|}{l+2}$. This contradicts (30) since $D_{l+1}(x,E) \subseteq F$. ∎

Remark. It is easy to translate the proposition to the case of an abelian group $\mathbb{G}$ written additively. Choose $\mathbb{G}$ to be the additive group of $\mathbb{Q}$. Let s be a positive integer, let $A = \{p_1, \ldots, p_s\}$ be a set of s distinct prime numbers, and let T be the A-equivalence class of 1 in $\mathbb{G} = \mathbb{Q}$. Then Proposition 6.1 applied to arbitrary subsets E and F of T with $\mathcal{O}(E) \subseteq F$ translates into Proposition 6.2 of [7], upon identifying $\mathbb{Z}^s$ with T under the map which sends a point $(i_1, \ldots, i_s) \in \mathbb{Z}^s$ to the rational number $p_1^{i_1} \cdots p_s^{i_s}$.

7. Estimates for the gcd. We now apply the combinatorial result of the preceding section to provide estimates for the degree and height of the greatest common divisor of a family of polynomials of the form $P(T^a)$ where P is fixed and a varies among a finite set A of integers. The result that we prove below implies Theorem 1.2.

THEOREM 7.1. *Let K be a number field, let $M, n \in \mathbb{N}^*$ with $M \geq 2$, let A be a non-empty set of prime numbers p from the interval $M/2 \leq p \leq M$, let P be a non-zero polynomial of $K[T]$ of degree at most n with no root in $\mathbb{C}^\times_{\mathrm{tor}} \cup \{0\}$, and let $Q \in K[T]$ be a greatest common divisor of the polynomials $P(T^a)$ with $a \in A$. Suppose that there exists an integer l satisfying*

$$4 \leq 2l \leq |A| \quad \text{and} \quad n \leq \frac{1}{2^{l+1}(l+1)!}\binom{|A|}{l+2}.$$

Then

$$\deg(Q) \leq \frac{6l}{|A|}\deg(P), \qquad \log H(Q) \leq \frac{c}{|A|M}\left(M\deg(P) + \log H(P)\right) \tag{37}$$

with $c = l\,2^{2l+6}$.

Proof. Suppose first that all roots of P are simple. Then, for each $a \in A$, the roots of $P(T^a)$ are also simple (since $P(0) \neq 0$), and so the roots of Q are simple. Define $\mathbb{G}$ to be the multiplicative group $\mathbb{C}^\times$ of $\mathbb{C}$, and let E and F denote respectively the sets of roots of Q and P. By hypothesis, we have $F \subset \mathbb{G} \setminus \mathbb{G}_{\mathrm{tor}}$ and $|F| \leq n$. Moreover, for any $x \in E$ and any $a \in A$, x is a root of $P(T^a)$ and so we have $x^a \in F$. In the notation of §6, this means that $E \subset \mathbb{G} \setminus \mathbb{G}_{\mathrm{tor}}$ and that $\mathcal{O}(E) \subseteq F$. If $E = \emptyset$, then Q is a constant and (37) holds. Otherwise, Proposition 6.1 provides us with an integer $r \geq 1$, a sequence of points $x_1, \ldots, x_r$ of E, and partitions $E = E_1 \amalg \cdots \amalg E_r$ and $F = F_1 \amalg \cdots \amalg F_{r+1}$ satisfying, for $i = 1, \ldots, r$,

$$E_i \subseteq C_l(x_i), \qquad F_i \subseteq \mathcal{O}(E_i), \qquad |F_i| \geq \frac{|A| - l}{2(l+1)}\,|E_i| \geq \frac{|A|}{6l}\,|E_i|. \tag{38}$$

Summing term by term the last inequalities for $i = 1, \ldots, r$, we obtain $|F| \geq |A|\,|E|/(6l)$ and so

$$\deg(Q) = |E| \leq \frac{6l}{|A|}\,|F| = \frac{6l}{|A|}\deg(P). \tag{39}$$

For each $i = 1, \ldots, r$ and each point $x \in E_i$, we have $x \in C_l(x_i)$ and so there exist $p_1, \ldots, p_l, q_1, \ldots, q_l \in A$ such that $x_i^{p_1 \cdots p_l} = x^{q_1 \cdots q_l}$. This gives $H(x_i)^{p_1 \cdots p_l} = H(x)^{q_1 \cdots q_l}$, and thus

$$2^{-l}\log H(x_i) \leq \log H(x) \leq 2^l \log H(x_i). \tag{40}$$

Combining this with the standard estimates (6) for the height of a polynomial in terms of the heights of its roots, and using (39), we deduce that

$$\begin{aligned} \log H(Q) &\leq \deg(Q) + \sum_{x \in E} \log H(x) \\ &\leq \frac{6l}{|A|}\deg(P) + \sum_{i=1}^{r} 2^l |E_i| \log H(x_i). \end{aligned} \tag{41}$$

On the other hand, for each $i = 1, \dots, r$ and each $y \in F_i$, we have $y \in \mathcal{O}(E_i)$ and so there exist $a \in A$ and $x \in E_i$ such that $y = x^a$. Then we get $H(y) = H(x)^a$, and by (40) we obtain

$$\log H(y) \geq \frac{M}{2} \log H(x) \geq \frac{M}{2^{l+1}} \log H(x_i).$$

Combining this with (6) and using (38), we find

$$\begin{aligned} \log H(P) + \deg(P) &\geq \sum_{y \in F} \log H(y) \geq \sum_{i=1}^{r} \frac{M}{2^{l+1}} |F_i| \log H(x_i) \\ &\geq \frac{|A|M}{6l\, 2^{l+1}} \sum_{i=1}^{r} |E_i| \log H(x_i). \end{aligned}$$

This provides an upper bound for $\sum_{i=1}^{r} |E_i| \log H(x_i)$ which after substitution into (41) leads to

$$\log H(Q) \leq \frac{c_1}{|A|M} \left(M \deg(P) + \log H(P)\right)$$

with $c_1 = l\, 2^{2l+4} \geq 6l(1 + 2^{2l+1})$. This proves the theorem with the constant c replaced by c_1 when P has only simple roots.

In the general case, let m denote the largest multiplicity of a root of P. For $i = 1, \dots, m$, let Z_i denote the set of roots of P having multiplicity at least i, and put $P_i = \prod_{x \in Z_i} (T - x)$. Since roots of P which are conjugate over K have the same multiplicity, $P_1, \dots, P_m$ are polynomials of $K[T]$. Moreover, they have simple roots and P is a constant multiple of their product $P_1 \cdots P_m$. Put $Q_i = \gcd\{P_i(T^a)\,; a \in A\}$ for $i = 1, \dots, m$. We claim that Q is a constant multiple of $Q_1 \cdots Q_m$.

To prove this claim, choose any root x of Q. We first observe that, for each $a \in A$, the multiplicity of x as a root of $P(T^a)$ is the same as the multiplicity of x^a as a root of P (since $T^a - x^a$ has only simple roots). Therefore the multiplicity of x as a root of Q is the largest integer i such that $\mathcal{O}(x) \subseteq Z_i$, or equivalently, it is the largest integer i such that x is a root of each of the polynomials $Q_1, \dots, Q_i$. This being true for each root x of Q shows that Q divides $Q_1 \cdots Q_m$. As the converse is clear, our claim follows.

Since $P_1, \dots, P_m$ all have degree at most n, the above considerations show that the estimates (37) apply to the pair (Q_i, P_i) for each $i = 1, \dots, m$, with c replaced by c_1. From this we deduce that

$$\deg(Q) = \sum_{i=1}^{m} \deg(Q_i) \leq \sum_{i=1}^{m} \frac{6l}{|A|} \deg(P_i) = \frac{6l}{|A|} \deg(P)$$

and

$$\begin{aligned}\log H(Q) &\le \deg(Q) + \sum_{i=1}^{m} \log H(Q_i)\\ &\le \deg(Q) + \sum_{i=1}^{m} \frac{c_1}{|A|M}\,(M\deg(P_i) + \log H(P_i))\\ &\le \frac{c_1}{|A|M}\,((2M+1)\deg(P) + \log H(P)),\end{aligned}$$

showing that (37) holds in general with $c = 4c_1$. ∎

8. Proof of Theorem 1.1 for rank at least two. Let the notation be as in Theorem 1.1, and suppose that $m \ge 2$. For $\sigma = 0$, the result follows from [5, Prop. 1]. So, we may assume that $\sigma > 0$. Define positive constants μ and ε by

$$\mu = \frac{m+1}{m+5}\,\sigma, \qquad \varepsilon = \frac{1}{8}\min\left\{\sigma - \mu,\ \nu - 1 - \beta + \frac{3m-1}{m+5}\,\sigma + \tau\right\}. \tag{42}$$

We proceed by contradiction, assuming on the contrary that for each sufficiently large value of n there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ with $\deg(P) \le n$ and $H(P) \le \exp(n^\beta)$ satisfying (4). Upon dividing P by its content, we may assume that P is primitive. Fix such an integer n and a corresponding polynomial P. Each computation below assumes that n is larger than an appropriate constant depending only on β, ε, μ, σ, τ, ν, $\xi_1, \dots, \xi_m$, a condition that we write, for short, as $n \gg 1$. Define

$$t = \left[\frac{n^\tau + 1}{2}\right], \qquad d = \left[\frac{n}{t}\right], \qquad \delta = \exp\left(-\frac{n^\nu}{6t}\right),$$
$$M = [n^\mu], \qquad N = [n^\sigma], \qquad X = \exp(n^\beta),$$

and factor P as a product $P(T) = T^r \Phi(T)^t P_0(T)$ where r is the largest non-negative integer such that T^r divides $P(T)$, and where Φ is the cyclotomic polynomial of $\mathbb{Z}[T]$ of largest degree such that Φ^t divides P. Since $\nu > 1$, the main condition (28) of Corollary 5.2 is satisfied for $n \gg 1$ and so there exist relatively prime positive integers $a_1, \dots, a_m, D$ with $D \le (2mn^{2+\sigma})^m$ and a proper subspace U of $\mathbb{Q}^m$ such that we have $|\Phi(\xi_1^{i_1} \cdots \xi_m^{i_m})| \ge \delta$ for any point $(i_1, \dots, i_m) \in \mathbb{Z}^m \setminus U$ satisfying $\max\{|i_1|, \dots, |i_m|\} \le n^\sigma$ and $\gcd(a_1 i_1 + \cdots + a_m i_m, D) = 1$. If $\xi_1, \dots, \xi_m$ do not all have absolute value one, we can further assume that $a_1 = \cdots = a_m = D = 1$ by applying Proposition 5.3 instead. Define

$$A = \{a \in \mathcal{P}\,;\, M/2 \le a \le M \text{ and } a \nmid D\}$$

where $\mathcal{P}$ denotes the set of all prime numbers, and define

$$E = \{\xi_1^{i_1} \cdots \xi_m^{i_m}\,;\, (i_1, \dots, i_m) \in I \setminus (U \cup U')\},$$

where U' denotes the proper subspace of $\mathbb{Q}^m$ generated by all the points $(i_1, \dots, i_m)$ of $\mathbb{Z}^m$ for which $\xi_1^{i_1} \cdots \xi_m^{i_m}$ is algebraic over $\mathbb{Q}$, and where

$$I = \{(i_1, \dots, i_m) \in \mathbb{Z}^m \,; 1 \le i_1, \dots, i_m \le n^{\sigma-\mu}, \\ \gcd(a_1 i_1 + \cdots + a_m i_m, D) = 1\}.$$

Then, in the notation of Proposition 3.1, we have both $\delta_\Phi \ge \delta$ and $\delta_P \le \exp(-n^\nu)$. We claim that for $n \gg 1$, we also have

$$n^{\mu-\varepsilon} \le |A| \le n^\mu \quad \text{and} \quad n^{m(\sigma-\mu)-\varepsilon} \le |E| \le n^{m(\sigma-\mu)}. \tag{43}$$

The upper bounds are clear and the lower bound for $|A|$ comes from the prime number theorem. The lower bound for $|E|$ follows from

$$|E| \ge |I| - |I \cap U| - |I \cap U'| \ge |I| - 2n^{(m-1)(\sigma-\mu)}$$

together with the fact that, by Lemma A.3 (in the Appendix), we have $|I| \ge 3n^{m(\sigma-\mu)-\varepsilon}$ for $n \gg 1$. In particular, both sets A and E are not empty. The main conditions (10) of Proposition 3.1 are also satisfied for $n \gg 1$ since we have

$$\tau + m(\sigma - \mu) < 1 + \mu \quad \text{and} \quad 1 + \mu < 1 + \sigma \le \beta.$$

Therefore, according to this proposition, the polynomial

$$Q(T) = \gcd\{P_0^{[j]}(T^a) \,; a \in A,\, 0 \le j < t\} \in \mathbb{Z}[T]$$

satisfies

$$\begin{aligned} \prod_{\xi \in E} \frac{|Q(\xi)|}{\operatorname{cont}(Q)} &\le X^{5Mn/t} \Delta_E^{-t} \left(\frac{\exp(-n^\nu)}{\delta^{3t}}\right)^{|E|} \\ &\le \exp(15 n^{1+\beta+\mu-\tau}) \Delta_E^{-t} \exp(-n^\nu |E|/2) \\ &\le \exp(15 n^{\nu+m(\sigma-\mu)-8\varepsilon}) \Delta_E^{-t} \exp(-n^\nu |E|/2). \end{aligned}$$

Since Q is primitive (being a divisor of $P(T^a)$ for any $a \in A$), we conclude from (43) that for $n \gg 1$ we have

$$\prod_{\xi \in E} |Q(\xi)| \le \exp\left(-\frac{n^\nu |E|}{4}\right) \Delta_E^{-t} = \prod_{\xi \in E} \left(\exp\left(-\frac{n^\nu}{4}\right) \prod_{\xi' \in E \setminus \{\xi\}} |\xi' - \xi|^{-t/2}\right).$$

Thus, there exists at least one point $\xi \in E$ such that

$$|Q(\xi)| \le \exp\left(-\frac{n^\nu}{8}\right) \quad \text{or} \quad \prod_{\xi' \in E \setminus \{\xi\}} |\xi' - \xi| \le \exp\left(-\frac{n^\nu}{4t}\right). \tag{44}$$

Suppose for the moment that the first inequality in (44) holds. Denote by P_1 a divisor of P in $\mathbb{Z}[T]$ of largest degree with no root in $\mathbb{C}_{\mathrm{tor}}^\times \cup \{0\}$, and define

$$Q_1 = \gcd\{P_1(T^a) \,; a \in A\} \in \mathbb{Z}[T].$$

As P_1 divides P in $\mathbb{Z}[T]$, we have both $\deg(P_1) \le n$ and $\log H(P_1) \le n + \log H(P) \le 2n^\beta$. Since P_1 has no root in $\mathbb{C}^\times_{\mathrm{tor}} \cup \{0\}$, and since $|A| \ge n^{\mu-\varepsilon} \ge n^{\mu/2}$ by (43), Theorem 7.1 applies for $n \gg 1$ with the choice of $l = [2/\mu]$, and it gives

$$\deg(Q_1) \le n^{1-\mu+2\varepsilon} \quad \text{and} \quad \log H(Q_1) \le n^{\beta-2\mu+2\varepsilon}.$$

We claim moreover that Q and Q_1 are related by

$$Q = \gcd\{Q_1^{[j]}(T)\,; 0 \le j < t\}.$$

As Q and Q_1 are primitive, this amounts to showing that their orders of vanishing at any point $z \in \mathbb{C}$ satisfy

$$\mathrm{ord}_z(Q) = \max\{0, \mathrm{ord}_z(Q_1) - t + 1\}. \tag{45}$$

To prove this, we first note that neither P_0 nor P_1 vanishes at $z = 0$. So the same is true for Q and Q_1, and thus both sides of (45) are 0 when $z = 0$. Assume from now on that $z \in \mathbb{C}^\times$. Then

$$\mathrm{ord}_z(Q) = \min_{a\in A} \max\{0, \mathrm{ord}_{z^a}(P_0) - t + 1\} \quad \text{and} \quad \mathrm{ord}_z(Q_1) = \min_{a\in A} \mathrm{ord}_{z^a}(P_1).$$

If $z \in \mathbb{C}^\times_{\mathrm{tor}}$, we have $\mathrm{ord}_{z^a}(P_0) < t$ and $\mathrm{ord}_{z^a}(P_1) = 0$ for each $a \in A$, and then both sides of (45) are again equal to 0. Otherwise, we find $\mathrm{ord}_{z^a}(P_0) = \mathrm{ord}_{z^a}(P_1)$ for each $a \in A$, and (45) follows.

The above discussion shows that we may apply Lemma 2.1 to the pair of polynomials Q and Q_1 with the function $\varphi\colon \mathbb{Z}[T] \to [0,\infty)$ given by $\varphi(F) = |F(\xi)|$, and the choice of parameters $d = n^{1-\mu+2\varepsilon}$, $Y = \exp(n^{\beta-2\mu+2\varepsilon})$ and $\delta = \exp(-n^\nu/8)$. Assuming $n \gg 1$, this lemma ensures the existence of a primary polynomial $S \in \mathbb{Z}[T]$ with

$$\deg(S) \le 4n^{1-\mu-\tau+2\varepsilon}, \quad \log H(S) \le 8n^{\beta-2\mu-\tau+2\varepsilon}, \quad |S(\xi)| \le \exp(-n^{\nu-\tau-\varepsilon}).$$

We have $S(\xi) \ne 0$ since $S \ne 0$ and since ξ is transcendental over $\mathbb{Q}$ (like all the elements of E). Write $\xi = \xi_1^{i_1} \cdots \xi_m^{i_m}$ with exponents in the range $1 \le i_1, \dots, i_m \le n^{\sigma-\mu}$. Then $\widetilde{S}(T_1, \dots, T_m) = S(T_1^{i_1} \cdots T_m^{i_m})$ is a polynomial of $\mathbb{Z}[T_1, \dots, T_m]$ which for $n \gg 1$ satisfies

$$\begin{aligned} \deg(\widetilde{S}) &\le n^{1+\sigma-2\mu-\tau+3\varepsilon}, \\ \log H(\widetilde{S}) &\le n^{\beta-2\mu-\tau+3\varepsilon}, \\ 0 < |\widetilde{S}(\xi_1, \dots, \xi_m)| &\le \exp(-n^{\nu-\tau-\varepsilon}). \end{aligned} \tag{46}$$

Suppose now that the second inequality holds in (44). Then

$$\prod_{\xi' \in E\setminus\{\xi\}} |\xi' - \xi| = \widetilde{S}(\xi_1, \dots, \xi_m)$$

with $\widetilde{S} \in \mathbb{Z}[T_1, \dots, T_m]$ satisfying $\deg(\widetilde{S}) \le mn^{\sigma-\mu}|E|$, $\log H(\widetilde{S}) \le |E|$ as well as the last inequality of (46) when $n \gg 1$. Since $(m+1)(\sigma-\mu) \le$

$1+\sigma-2\mu-\tau$, we deduce that $\widetilde{S}$ also satisfies the first two inequalities of (46) when $n \gg 1$.

Therefore the constraints (46) have a solution $\widetilde{S} \in \mathbb{Z}[T_1, \dots, T_m]$ for each $n \gg 1$. This contradicts Lemma 2.3 (Gel'fond's criterion) since $\beta \geq 1+\sigma$ and since the choice of ε in (42) implies

$$\nu - \tau - \varepsilon \geq (1+\sigma-2\mu-\tau+3\varepsilon) + (\beta-2\mu-\tau+3\varepsilon) + \varepsilon.$$

The proof is complete. ∎

9. Avoiding cyclotomic factors in rank one. The rest of this paper is devoted to the proof of Theorem 1.1 in the case where $m = 1$. In this section, we first establish a measure of approximation of a complex number ξ by roots of unity, under conditions that are sensibly weaker than those of Theorem 1.1. We then prove two corollaries which finally allow us to push forward the conclusion of Proposition 3.1. The reader who simply wants a proof of Theorem 1.1 in the case where $m = 1$ and $|\xi_1| \neq 1$ can go directly to the Remark following those two corollaries and then proceed to Proposition 9.4 at the end of the section.

PROPOSITION 9.1. *Let $\xi \in \mathbb{C}^\times \setminus \mathbb{C}^\times_{\mathrm{tor}}$, and let $\beta, \sigma, \tau, \nu \in \mathbb{R}$ with*

$$\sigma > 0, \quad \tau \geq 0, \quad \sigma + \tau \leq 1 \leq \beta \quad \text{and} \quad \nu > 1 + \beta - \sigma - \tau.$$

Suppose that, for each sufficiently large positive integer n, there exists a non-zero polynomial $P = P_n \in \mathbb{Z}[T]$ with $\deg(P) \leq n$ and $H(P) \leq \exp(n^\beta)$ satisfying

$$\max\{|P^{[j]}(\xi^i)|\,; 1 \leq i \leq n^\sigma,\ 0 \leq j < n^\tau\} \leq \exp(-n^\nu).$$

Then the ratio $\varrho = (\nu-\tau)/(1-\tau)$ is a real number with $\varrho > 1$ and, for each sufficiently large positive integer D and each root of unity Z of order D, we have

$$|\xi - Z| \geq \exp(-\phi(D)^\varrho).$$

Proof. We have $\varrho > 1$ because $\nu > 1 > \tau$. Now, suppose on the contrary that there exist roots of unity Z of arbitrarily large order D with $|\xi - Z| < \exp(-\phi(D)^\varrho)$. Fix such a pair D and Z and put $m = \phi(D)$. By taking D large enough, we may assume that the integer n determined by the condition

$$2n^{1-\tau} < m \leq 2(n+1)^{1-\tau}$$

is arbitrarily large. In particular, we may assume that there exists a corresponding polynomial $P = P_n \in \mathbb{Z}[T]$. Furthermore, we may assume that P is primitive, so that $H(P) = \|P\|$. Let $j \geq 0$ be the smallest non-negative integer such that $P^{(j)}(Z) \neq 0$. Since Z has degree m over $\mathbb{Q}$, we have $jm \leq \deg(P) \leq n$ and so $j \leq n/m < n^\tau/2$. Consider the polynomial $Q = P^{[j]} \in \mathbb{Z}[T]$. It has degree $\deg(Q) \leq n$ and length $L(Q) \leq$

$(n+1)2^n\|P\| \le \exp(3n^\beta)$. Since $Q(Z)$ is a non-zero algebraic integer of $\mathbb{Q}(Z)$, its norm from $\mathbb{Q}(Z)$ to $\mathbb{Q}$ is a non-zero integer and so

$$1 \le \prod_{\substack{1\le i\le D\\ \gcd(i,D)=1}} |Q(Z^i)|. \tag{47}$$

Let I denote the set of all integers i coprime to D with $1 \le i \le n^\sigma$. Since $D \ge m > 2n^{1-\tau} \ge 2n^\sigma$, this is a subset of the indexing set of the product on the right hand side of (47). For each $i \in I$, we use the Taylor expansion of Q around ξ^i to estimate $|Q(Z^i)|$. Fix such an index i. This gives

$$|Q(Z^i)| \le \sum_{k=0}^{\infty} |Q^{[k]}(\xi^i)|\,|\xi^i - Z^i|^k.$$

Since $m > 2n^{1-\tau}$ and $\varrho > 1$, we have $|\xi - Z| < \exp(-m^\varrho) < \exp(-2n^{\nu-\tau})$. If n is sufficiently large, we also have $\exp(-2n^{\nu-\tau}) \le n^{-\sigma}$, therefore $|\xi| \le 1 + n^{-\sigma}$, and so $\max\{1,|\xi|\}^i \le e$ since $i \le n^\sigma$. Combining these estimates, we obtain, for n sufficiently large,

$$|\xi^i - Z^i| = |\xi - Z|\Big|\sum_{l=0}^{i-1} \xi^l Z^{i-l-1}\Big| \le \exp(-2n^{\nu-\tau})n^\sigma e \le \exp(-n^{\nu-\tau}).$$

In particular, we may assume that $|\xi^i - Z^i| \le 1/2$. On the other hand, since $j < n^\tau/2$, we have $j + k < n^\tau$ for any integer k with $0 \le k \le n^\tau/2$, and for such an integer k the hypothesis on P leads to

$$|Q^{[k]}(\xi^i)| = \binom{j+k}{j}|P^{[j+k]}(\xi^i)| \le 2^n \exp(-n^\nu).$$

For the remaining integers $k > n^\tau/2$, we use instead the crude estimate

$$|Q^{[k]}(\xi^i)| \le \max\{1,|\xi^i|\}^n L(Q^{[k]}) \le e^n 2^n L(Q) \le \exp(5n^\beta).$$

So, putting all together, we find for each $i \in I$ that

$$\begin{aligned}
|Q(Z^i)| &\le 2^n \exp(-n^\nu) \sum_{k=0}^{[n^\tau/2]} |\xi^i - Z^i|^k + \exp(5n^\beta) \sum_{k=[n^\tau/2]+1}^{\infty} |\xi^i - Z^i|^k \\
&\le 2^{n+1} \exp(-n^\nu) + 2\exp(5n^\beta)|\xi^i - Z^i|^{n^\tau/2} \\
&\le 2^{n+1} \exp(-n^\nu) + 2\exp(5n^\beta - n^\nu/2) \\
&\le \exp(-n^\nu/3),
\end{aligned}$$

where the last step again assumes that n is sufficiently large. For all the other integers i, we use

$$|Q(Z^i)| \le L(Q) \le \exp(3n^\beta).$$

Since the inequality (47) involves a product of m factors of the form $|Q(Z^i)|$, including those with $i \in I$, we deduce that

$$1 \le \exp(3n^\beta)^m \exp(-n^\nu/3)^{|I|}. \tag{48}$$

Define $\varepsilon = (1/2)(\nu - 1 - \beta + \sigma + \tau) > 0$. We have $m \le 2(n+1)^{1-\tau} \le 4n^{1-\tau}$, and Lemma A.3 (or the prime number theorem) gives $|I| \ge n^{\sigma-\varepsilon}$ for n sufficiently large, since $D = \mathcal{O}(m^2) = \mathcal{O}(n^2)$. Substituting these estimates for m and $|I|$ into (48) leads to a contradiction, as $\beta + 1 - \tau < \nu + \sigma - \varepsilon$. ∎

Corollary 9.2. *Under the notation and hypotheses of Proposition* 9.1, *there exists a positive integer n_1 with the following property. For each pair of integers n and t with $n \ge n_1$ and $t \ge n^\tau/3$, and for each cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ whose tth power Φ^t divides the polynomial $P = P_n$, there exists a positive integer D with $D \le 2n^3$ such that*

$$\min\{|\Phi(\xi^i)|\,; 1 \le i \le n^\sigma,\ \gcd(i, D) = 1\} \ge \exp\left(-\frac{n^\nu}{6t}\right). \tag{49}$$

Proof. Choose $\varepsilon > 0$ such that $\nu - \varepsilon > 1 + \beta - \sigma - \tau$. Then the hypotheses of Proposition 9.1 remain satisfied with the parameter ν replaced by $\nu - \varepsilon$, and so there exists a constant $c > 0$ such that, for any integer $D \ge 1$ and any root of unity Z of order D, we have

$$|\xi - Z| \ge \exp(-c\phi(D)^{\widetilde{\varrho}}) \quad \text{where} \quad \widetilde{\varrho} = \frac{\nu - \varepsilon - \tau}{1 - \tau}. \tag{50}$$

Let n be a positive integer for which the polynomial $P = P_n$ is defined, let t be an integer with $t \ge n^\tau/3$, and let Φ be a cyclotomic polynomial of $\mathbb{Z}[T]$ such that Φ^t divides P. We may assume that Φ is non-constant, and so we have $t \le n$. Then, for n sufficiently large, all conditions of Proposition 4.1 are satisfied with $m = 1$, $\xi_1 = \xi$ and the choice of parameters $d = [n/t]$, $\delta = \exp(-n^\nu/(6t))$ and $N = [n^\sigma]$ (the condition (14) holds since $\nu > 1$). So, there exist relatively prime positive integers a_1 and D with $D \le 2(n/t)^2 n^\sigma \le 2n^3$ such that either (49) holds or there exists a root Z of Φ which has order D as a root of unity and satisfies

$$|\xi - Z^{a_1}|^G \le \exp\left(-\frac{n^\nu}{12t}\right) \tag{51}$$

where G denotes the multiplicity of Z as a root of Φ. Suppose that the second eventuality holds. We will see that, in this case, the integer n is bounded and this will complete the proof. Since Z and Z^{a_1} are conjugate over $\mathbb{Q}$ (they have the same order D), we may assume without loss of generality that $a_1 = 1$. Then, by comparing (50) and (51), we find

$$cG\phi(D)^{\widetilde{\varrho}} \ge \frac{n^\nu}{12t}. \tag{52}$$

However, since Z has degree $\phi(D)$ over $\mathbb{Q}$, we also have $G\phi(D) \le \deg(\Phi) \le n/t$. Combining this with (52), we get $12c\phi(D)^{\widetilde{\varrho}-1} \ge n^{\nu-1}$. Finally, since $\phi(D) \le n/t \le 3n^{1-\tau}$, this gives $n \le (12c\,3^{\widetilde{\varrho}-1})^{1/\varepsilon}$. ∎

COROLLARY 9.3. *Let the notation and hypotheses be as in Proposition* 9.1, *and let* $\mu \in \mathbb{R}$ *with* $0 < \mu \le 1-\tau$ *and* $2\mu+\tau < \nu$. *Then there exists a positive integer* n_2 *with the following property. For each integer* $n \ge n_2$ *and each non-empty subset* I *of* $\{1,\dots,[n^\mu]\}$, *the set* $E = \{\xi^i\,; i \in I\}$ *satisfies*

$$\Delta_E \ge \exp\Big(-\frac{1}{4}\,n^{\nu-\tau}|E|\Big).$$

Proof. Again, choose $\varepsilon > 0$ such that $\nu - \varepsilon > 1 + \beta - \sigma - \tau$. Arguing as in the proof of Corollary 9.2, we find that there is a constant $c > 0$ such that (50) holds for any integer $D \ge 1$ and any root of unity Z of order D. Let n be a positive integer and let $E = \{\xi^i\,; i \in I\}$ for some non-empty subset I of $\{1,\dots,[n^\mu]\}$. Suppose that $\Delta_E < \exp(-(1/4)n^{\nu-\tau}|E|)$. We need to show that n is bounded (independently of the choice of I). By definition, we have $\Delta_E = \prod_{i<j} |\xi^i - \xi^j|$ where the product runs through all pairs (i,j) of elements of I with $i < j$. This means that we can write $\Delta_E = |\xi|^r\,|\Phi(\xi)|$ for an integer r with $0 \le r \le n^{2\mu}|E|$ and a cyclotomic polynomial Φ of $\mathbb{Z}[T]$ of degree at most $n^{2\mu}|E|$. Applying Lemma 4.4, we deduce that some root Z of Φ satisfies

$$|\xi - Z|^G \le \exp\Big(n^{2\mu}|E|\log(c_1(n^{3\mu})^4) - \frac{1}{4}\,n^{\nu-\tau}|E|\Big),$$

where $c_1 = 2\max\{1, |\xi|^{-1}\}$ and where G denotes the multiplicity of Z as a root of Φ. Since $\nu - \tau > 2\mu$, we conclude that for n large enough we have

$$|\xi - Z|^G \le \exp\Big(-\frac{1}{8}\,n^{\nu-\tau}|E|\Big). \tag{53}$$

Now, let D denote the order of Z as a root of unity. Combining (53) with (50), we obtain

$$8cG\phi(D)^{\widetilde{\varrho}} \ge n^{\nu-\tau}|E|. \tag{54}$$

On the other hand, by the actual definition of Φ, we have $D \le n^\mu$, and G is the number of pairs of elements (i,j) of I with $i < j$ and $i \equiv j \bmod D$. Thus, we also have $G \le n^\mu|E|/D$. Substituting this upper bound for G into (54) and using $\phi(D) \le D$, we obtain $8cD^{\widetilde{\varrho}-1} \ge n^{\nu-\mu-\tau}$. Finally, since $D \le n^\mu \le n^{1-\tau}$, this leads to $8cn^{\nu-1-\varepsilon} \ge n^{\nu-\mu-\tau}$, thus $8c \ge n^{1+\varepsilon-\mu-\tau} \ge n^\varepsilon$ and so $n \le (8c)^{1/\varepsilon}$. ∎

REMARK. If we assume that $|\xi| \ne 1$, then for each cyclotomic polynomial $\Phi \in \mathbb{Z}[T]$ and each non-zero integer i, we find

$$|\Phi(\xi^i)| \ge \big|1 - |\xi^i|\big|^{\deg(\Phi)} \ge c_1^{\deg(\Phi)},$$

where $c_1 = 1 - \min\{|\xi|, |\xi|^{-1}\}$. Since $\nu > 1$, we deduce that, in this case, Corollary 9.2 holds with $D = 1$. Moreover, for a set E as in Corollary 9.3, we have $\Delta_E = |\xi|^r \Phi(\xi)$ where r is an integer with $0 \le r \le n^{2\mu}|E|$ and Φ is a cyclotomic polynomial of $\mathbb{Z}[T]$ with $\deg(\Phi) \le n^{2\mu}|E|$, and thus $\Delta_E \ge \exp(c_2 n^{2\mu}|E|)$ where $c_2 = \log(c_1 \min\{1, |\xi|\})$, which is stronger than the conclusion of Corollary 9.3.

The main result of this section is the following.

PROPOSITION 9.4. *Let $\xi \in \mathbb{C}^\times \setminus \mathbb{C}^\times_{\mathrm{tor}}$, and let $\beta, \varepsilon, \mu, \sigma, \tau, \nu \in \mathbb{R}$ with*

$$0 < \mu < \sigma, \quad 0 \le \tau \le 1 - \sigma, \quad \beta > \max\{1 + \sigma - \mu, 2\mu + \tau\},$$
$$0 < 2\varepsilon < \min\{\mu, \sigma - \mu\} \quad \text{and} \quad \nu > 1 + \beta + \sigma - 2\mu - \tau + 2\varepsilon.$$

Suppose that for each sufficiently large positive integer n, there exists a non-zero polynomial $P = P_n \in \mathbb{Z}[T]$ with $\deg(P) \le n$ and $H(P) \le \exp(n^\beta)$ satisfying

$$\max\{|P^{[j]}(\xi^i)| \,;\, 1 \le i \le n^\sigma,\ 0 \le j < n^\tau\} < \exp(-n^\nu).$$

Then, for each large enough index n, there exists a positive integer D with $D \le 2n^3$ and with the following property. For any set I of cardinality $|I| \ge n^{\mu-\varepsilon}$ consisting of integers i coprime to D in the range $1 \le i \le n^\mu$, there exists a primary polynomial $S \in \mathbb{Z}[T]$ satisfying

$$\deg(S) \le n^{1-(\sigma-\mu)-\tau+3\varepsilon}, \quad \log H(S) \le n^{\beta-2(\sigma-\mu)-\tau+3\varepsilon},$$
$$\prod_{i \in I} |S(\xi^i)| \le \exp(-n^{\nu+\mu-\tau-2\varepsilon}). \tag{55}$$

Proof. Fix a large integer n and a corresponding polynomial P. Without loss of generality, we may assume that P is primitive. Put $t = [(n^\tau + 1)/2]$, and write $P(T)$ as a product $P(T) = T^r \Phi(T)^t P_0(T)$, where r is the largest positive integer such that T^r divides P and Φ is the cyclotomic polynomial of $\mathbb{Z}[T]$ of largest degree such that Φ^t divides P. Assuming n large enough, Corollary 9.2 shows that (49) holds for some integer D with $1 \le D \le 2n^3$. Let I be a subset of $\{i \in \mathbb{Z} \,;\, 1 \le i \le n^\mu, \gcd(i, D) = 1\}$ with cardinality $|I| \ge n^{\mu-\varepsilon}$ (such a subset exists if n is large enough), and form the set $E = \{\xi^i \,;\, i \in I\}$. Put also $M = [n^{\sigma-\mu}]$ and define A to be the set of all prime numbers p not dividing D with $M/2 \le p \le M$. Finally, set $X = \exp(n^\beta)$ so that $H(P) \le X$. Then, in the notation of Proposition 3.1, we have

$$c_E \le \exp(c_1 n^\mu), \quad \delta_\Phi \ge \exp\left(-\frac{n^\nu}{6t}\right) \quad \text{and} \quad \delta_P \le \exp(-n^\nu),$$

where $c_1 = \log \max\{|\xi|, |\xi|^{-1}\}$. Since $\xi \notin \mathbb{C}^\times_{\mathrm{tor}} \cup \{0\}$, the sets E and I have the same cardinality. Assuming n large enough, we have

$$n^{\sigma-\mu-\varepsilon} \le |A| \le n^{\sigma-\mu} \quad \text{and} \quad n^{\mu-\varepsilon} \le |E| = |I| \le n^\mu$$

and the main condition (10) of Proposition 3.1 holds because $\tau + \mu < 1 + \sigma - \mu < \beta$ and $2\mu + \tau < \beta$. Combining that proposition with Corollary 9.3, we deduce that the polynomial

$$Q(T) = \gcd\{P_0^{[j]}(T^a)\,;\, a \in A,\, 0 \le j < t\} \in \mathbb{Z}[T]$$

satisfies

$$\prod_{i\in I} |Q(\xi^i)| \le \exp\left(\frac{5}{t}\, n^{1+\beta+\sigma-\mu}\right) \Delta_E^{-t} \exp\left(-\frac{n^\nu}{2}\,|E|\right)$$
$$\le \exp(15n^{1+\beta+\sigma-\mu-\tau}) \exp\left(-\frac{n^\nu}{4}\,|E|\right) \le \exp\left(-\frac{1}{8}\, n^{\nu+\mu-\varepsilon}\right)$$

provided that n is large enough.

Denote by P_1 a divisor of P in $\mathbb{Z}[T]$ of largest degree with no root in $\mathbb{C}_{\mathrm{tor}}^\times \cup \{0\}$, and define

$$Q_1 = \gcd\{P_1(T^a)\,;\, a \in A\} \in \mathbb{Z}[T].$$

Applying Theorem 7.1 as in Section 8, upon noting that $\beta \ge 1 + \sigma - \mu$, we find that for n sufficiently large we have

$$\deg(Q_1) \le n^{1-(\sigma-\mu)+2\varepsilon} \quad \text{and} \quad \log H(Q_1) \le n^{\beta-2(\sigma-\mu)+2\varepsilon}.$$

As in Section 8, we also note that $Q = \gcd\{Q_1^{[j]}(T)\,;\, 0 \le j < t\}$. This means that we may apply Lemma 2.1 to the pair of polynomials Q and Q_1 with the function $\varphi\colon \mathbb{Z}[T] \to [0,\infty)$ given by $\varphi(F) = \prod_{i\in I} |F(\xi^i)|$, and the choice of parameters

$$d = n^{1-(\sigma-\mu)+2\varepsilon}, \quad Y = \exp(n^{\beta-2(\sigma-\mu)+2\varepsilon}) \quad \text{and} \quad \delta = \exp(-(1/8)n^{\nu+\mu-\varepsilon}).$$

Assuming n large enough, this lemma ensures the existence of a primary polynomial $S \in \mathbb{Z}[T]$ with the required properties (55). ∎

10. An estimate related to Zarankiewicz problem. The following result is a strengthening of Proposition 9.1 of [7]. As the latter, it has connection with a well-known combinatorial problem of Zarankiewicz (see [3, Chap. 12]).

PROPOSITION 10.1. *Let A and B be finite non-empty sets, let κ_1 and κ_2 be positive real numbers, and let $\varphi\colon A \times B \to [0,\kappa_1]$ be any function on $A \times B$ with values in the interval $[0,\kappa_1]$. Suppose that the inequality*

$$\sum_{b\in B} \min\{\varphi(a_1,b), \varphi(a_2,b)\} \le \kappa_2$$

holds for any pair of distinct elements a_1 and a_2 of A. Then

$$\sum_{a\in A}\sum_{b\in B} \varphi(a,b) \le \max\{|A|\sqrt{2|B|\kappa_1\kappa_2}, 2|B|\kappa_1\}.$$

The connection with the problem of Zarankiewicz is the following. For positive integers m and n, an $m \times n$ matrix M with coefficients in $\{0,1\}$ can be viewed as a function $\varphi\colon A \times B \to \{0,1\}$ where $A = \{1,\dots,m\}$ and $B = \{1,\dots,n\}$. If, for some integer $n_1 \geq 1$, the matrix M contains no $2 \times n_1$ submatrix consisting entirely of ones, the hypotheses of the proposition are satisfied with $\kappa_1 = 1$ and $\kappa_2 = n_1 - 1$ and consequently this matrix contains at most $\max\{m\sqrt{2n(n_1-1)},\, 2n\}$ ones.

Proof of Proposition 10.1. We first claim that for each $i = 1,\dots,|A|$, we have

$$\sum_{a\in A}\sum_{b\in B}\varphi(a,b) \leq \frac{|A|\,|B|}{i}\,\kappa_1 + \frac{(i-1)|A|}{2}\,\kappa_2. \tag{56}$$

In the case where $i = |A|$, this follows from Proposition 9.1 of [7]. The proof of the general case proceeds by reduction to this situation. Put $m = |A|$ and, for each $a \in A$, define $\psi(a) = \sum_{b\in B}\varphi(a,b)$. Choose also an ordering $\{a_1,\dots,a_m\}$ of A such that $\psi(a_1) \geq \cdots \geq \psi(a_m)$, and consider the set $A' = \{a_1,\dots,a_i\}$. Then A' and B satisfy all the hypotheses of the proposition for the restriction of φ to $A' \times B$, with the same values of κ_1 and κ_2. Accordingly, by [7, Prop. 9.1], we have

$$\sum_{a\in A'}\psi(a) = \sum_{a\in A'}\sum_{b\in B}\varphi(a,b) \leq |B|\kappa_1 + \binom{i}{2}\kappa_2.$$

On the other hand, since $\psi(a_j) \leq (1/i)\sum_{a\in A'}\psi(a)$ for each $j = i+1,\dots,m$, we also find

$$\sum_{a\in A}\sum_{b\in B}\varphi(a,b) = \sum_{a\in A}\psi(a) \leq \left(1 + \frac{m-i}{i}\right)\sum_{a\in A'}\psi(a) = \frac{|A|}{i}\sum_{a\in A'}\psi(a).$$

Our claim (56) follows by combining these two estimates.

To conclude, put $\varrho = 2|B|\kappa_1/\kappa_2$. If $\varrho < |A|^2$, we apply the inequality (56) with $i = [\sqrt{\varrho}] + 1$. This gives

$$\sum_{a\in A}\sum_{b\in B}\varphi(a,b) \leq \frac{|A|\,|B|}{\sqrt{\varrho}}\,\kappa_1 + \frac{|A|\sqrt{\varrho}}{2}\,\kappa_2 = |A|\sqrt{\varrho}\,\kappa_2 = |A|\sqrt{2|B|\kappa_1\kappa_2}.$$

If $\varrho \geq |A|^2$, the same inequality with $i = |A|$ leads to

$$\sum_{a\in A}\sum_{b\in B}\varphi(a,b) \leq |B|\kappa_1 + \frac{|A|^2}{2}\,\kappa_2 \leq |B|\kappa_1 + \frac{\varrho}{2}\,\kappa_2 = 2|B|\kappa_1.$$

The proof is complete. ∎

11. Products of values of polynomials at powers of ξ. In this section, we use Proposition 10.1 to prove a transcendence criterion for a complex number ξ, based on products of values of polynomials at powers

of ξ. Then we combine this criterion with Proposition 9.4 to complete the proof of Theorem 1.1 in the case $m = 1$.

THEOREM 11.1. *Let $\xi \in \mathbb{C}$ be transcendental over $\mathbb{Q}$, and let $\alpha, \beta, \mu, \omega$ be in $\mathbb{R}$ with*

$$\alpha \geq \mu > 0, \quad \beta \geq \alpha + \mu \quad \text{and} \quad \omega > \alpha + \beta + (3/2)\mu. \tag{57}$$

For infinitely many positive integers n, there exists no primary polynomial $Q \in \mathbb{Z}[T]$ without root in $\mathbb{C}_{\mathrm{tor}}^{\times} \cup \{0\}$, satisfying

$$\deg(Q) \leq n^{\alpha}, \quad H(Q) \leq \exp(n^{\beta}), \quad \prod_{a \in A} \prod_{b \in B} |Q(\xi^{ab})| \leq \exp(-n^{\omega}) \tag{58}$$

for some non-empty subsets A and B of $\{1, \dots, [n^{\mu/2}]\}$.

Proof. We proceed by contradiction, assuming on the contrary that such a triple (Q, A, B) exists for each sufficiently large n. Fix an appropriate integer n, and define $E = \{\xi^b \,;\, b \in B\}$ for a corresponding choice of (Q, A, B). Note that Q is primitive being primary and non-constant, thus $H(Q) = \|Q\|$. We consider two cases according to the size of Δ_E (see §2 for the definition of this quantity).

CASE 1: $\Delta_E^{-1} \leq \exp((1/4)n^{\omega-\mu})$. We claim that, if n is sufficiently large, there exists $(a, b) \in A \times B$ such that $|Q(\xi^{ab})| \leq \exp(-(1/2)n^{\omega-\mu/2})$. To prove this, we first note that, for each $(a, b) \in A \times B$, we have

$$|Q(\xi^{ab})| \leq \|Q\| \exp(c_1 n^{\alpha+\mu}) \leq \exp((c_1 + 1)n^{\beta}),$$

where $c_1 = \log(1 + |\xi|)$, so that we can write

$$|Q(\xi^{ab})| = \exp((c_1 + 1)n^{\beta} - \varphi(a, b))$$

for some real number $\varphi(a, b) \geq 0$. This defines a function $\varphi\colon A \times B \to [0, \infty)$ which, by the last condition of (58), satisfies

$$\sum_{a \in A} \sum_{b \in B} \varphi(a, b) \geq n^{\omega}. \tag{59}$$

We also note that, for distinct elements a_1 and a_2 of A, the polynomials $Q(T^{a_1})$ and $Q(T^{a_2})$ are relatively prime in $\mathbb{Z}[T]$. This is because they are primitive polynomials of $\mathbb{Z}[T]$, and if z is a common root of them, then z^{a_1} and z^{a_2} are roots of $Q(T)$. However, since $Q(T)$ is a primary polynomial of $\mathbb{Z}[T]$, its roots are conjugate over $\mathbb{Q}$. So, there exists an automorphism σ of the splitting field of $Q(T)$ over $\mathbb{Q}$ such that $\sigma(z^{a_1}) = z^{a_2}$. Then, upon denoting by m the order of σ, we find $z^{a_1^m} = \sigma^m(z^{a_1^m}) = z^{a_2^m}$. Since $a_1^m \neq a_2^m$, this implies that $z \in \mathbb{C}_{\mathrm{tor}}^{\times} \cup \{0\}$, contrary to the assumption that $Q(T)$ has no root in that set. Thus, the gcd of $Q(T^{a_1})$ and $Q(T^{a_2})$ in $\mathbb{Z}[T]$ is 1.

We apply Proposition 2.2 to the above situation with $t = 1$, $r = 2$ and $P_i(T) = Q(T^{a_i})$ for $i = 1, 2$. Since both polynomials P_1 and P_2 have

degree $\le n^{\alpha+\mu/2}$ and height $\le \exp(n^\beta)$, and since we assume that $\Delta_E^{-1} \le \exp((1/4)n^{\omega-\mu})$, it gives

$$1 \le \exp(10n^{2\alpha+\mu} + c_2 n^{\alpha+3\mu/2} + (1/4)n^{\omega-\mu} + 2n^{\beta+\alpha+\mu/2}) \times \prod_{b\in B} \max\{\exp((c_1+1)n^\beta - \varphi(a_1,b)), \exp((c_1+1)n^\beta - \varphi(a_2,b))\},$$

where $c_2 = 4\log(2+|\xi|)$. By (57), the exponent $\omega-\mu$ exceeds all the other exponents of powers of n in the first factor on the right. So, if n is sufficiently large, we deduce that

$$\sum_{b\in B} \min\{\varphi(a_1,b), \varphi(a_2,b)\} \le \frac{1}{2}\, n^{\omega-\mu}.$$

This means that Proposition 10.1 applies to the function φ with κ_1 equal to the largest value of φ on $A\times B$, and with $\kappa_2 = (1/2)n^{\omega-\mu}$. Because of (59), this implies that

$$n^\omega \le \max\{n^{\mu/2}\sqrt{n^{\omega-\mu/2}\kappa_1}, 2n^{\mu/2}\kappa_1\},$$

and so $\kappa_1 \ge (1/2)n^{\omega-\mu/2}$. Thus, there exists $(a,b) \in A\times B$ such that

$$|Q(\xi^{ab})| \le \exp((c_1+1)n^\beta - (1/2)n^{\omega-\mu/2}).$$

If n is sufficiently large, this means that $|Q(\xi^{ab})| \le \exp(-(1/4)n^{\omega-\mu/2})$, thereby proving our claim. For such a choice of (a,b), the polynomial $S(T) = Q(T^{ab}) \in \mathbb{Z}[T]$ satisfies

$$\deg(S) \le n^{\alpha+\mu},\ H(S) \le \exp(n^\beta),\ 0 < |S(\xi)| \le \exp(-(1/4)n^{\omega-\mu/2}). \tag{60}$$

Case 2: $\Delta_E^{-1} > \exp((1/4)n^{\omega-\mu})$. In this situation, we define

$$S(T) = \prod_{\substack{b,b'\in B\\ b<b'}} |T^{b'} - T^b|^u \quad \text{where} \quad u = [n^{\mu/2}] + 1.$$

This polynomial of $\mathbb{Z}[T]$ satisfies the inequalities (60) because

$$\deg(S) \le \binom{|B|}{2} n^{\mu/2} u \le n^{2\mu} \le n^{\alpha+\mu},$$

$$\log H(S) \le \binom{|B|}{2} u\log(2) \le n^{3\mu/2} \le n^\beta,$$

and, by definition of Δ_E, we have $0 < |S(\xi)| = \Delta_E^u \le \exp(-(1/4)n^{\omega-\mu/2})$.

Thus, in both cases, the conditions (60) have a solution $S(T) \in \mathbb{Z}[T]$ for n sufficiently large. By Gel'fond's criterion (Lemma 2.3), this is impossible because $\beta \ge \alpha+\mu$ and $\omega - \mu/2 > (\alpha+\mu)+\beta$. ∎

Proof of Theorem 1.1 in the case $m = 1$. Suppose that the hypotheses of Theorem 1.1 are satisfied for $m = 1$. For $\sigma = 0$, the result follows from [5, Prop. 1]. We may therefore assume that $\sigma > 0$. Arguing by contradiction,

we also assume that, for each sufficiently large positive integer n, there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ with $\deg(P) \le n$ and $H(P) \le \exp(n^\beta)$ satisfying (4). Put $\xi = \xi_1$ and $\mu = (8/11)\sigma$. Then, the conditions of Proposition 9.4 are satisfied for any choice of $\varepsilon > 0$ small enough as a function of β, σ, τ, ν. For each sufficiently large n and for the corresponding integer D with $1 \le D \le 2n^3$ provided by Proposition 9.4, consider the set of all prime numbers p not dividing D in the interval $1 < p \le n^{\mu/2}$, and partition this set into two disjoint subsets A and B of cardinality at least $n^{(\mu-\varepsilon)/2}$. Then the set $I = \{ab\,; a \in A,\, b \in B\}$ has cardinality $|I| = |A|\,|B| \ge n^{\mu-\varepsilon}$ and consists of integers coprime to D from the interval $[1, n^\mu]$. So, Proposition 9.4 provides us with a primary polynomial $S \in \mathbb{Z}[T]$ satisfying the conditions (55). This contradicts Theorem 11.1 if, from the start, we choose ε small enough so that the conditions (57) hold with $\alpha = 1-(\sigma-\mu)-\tau+3\varepsilon$, $\omega = \nu+\mu-\tau-2\varepsilon$, and β replaced by $\beta-2(\sigma-\mu)-\tau+3\varepsilon$. ∎

Appendix. Counting lemmas. The purpose of this appendix is to provide an estimate that is needed in §8 in the course of the proof of the main Theorem 1.1 for the case $m \ge 2$. It concerns the cardinality of certain subsets of $\mathbb{Z}^m$ which arise from an application of Corollary 5.2. I believe that this has appeared elsewhere but as I have been unable to find a suitable reference, I include the details of the proof for the convenience of the reader. It starts with a preliminary lemma.

LEMMA A.1. *Let $m, d, N \in \mathbb{N}^*$, and let $a_1, \dots, a_m, b \in \mathbb{Z}$ be integers with $\gcd(a_1, \dots, a_m, d) = 1$. Then the set*

$$I = \{(i_1, \dots, i_m) \in \mathbb{Z}^m\,; 1 \le i_1, \dots, i_m \le N,\ a_1 i_1 + \cdots + a_m i_m \equiv b \bmod d\}$$

has cardinality $|I| = N^m/d + E$ with an error E satisfying $|E| \le (3N)^{m-1}$.

The crucial point here is that the error term depends only on m and N.

Proof. If $m = 1$, the set I is the intersection of $\{1, \dots, N\}$ with an arithmetic progression with difference d. Therefore, its cardinality is either $[N/d]$ or $[N/d]+1$, and so we have $\big||I| - N/d\big| \le 1$. Suppose now that $m \ge 2$. Write $d_1 = \gcd(a_1, d)$, $d' = d/d_1$ and $a' = a_1/d_1$, and define

$$I' = \{(i_2, \dots, i_m) \in \mathbb{Z}^{m-1}\,; 1 \le i_2, \dots, i_m \le N,\ a_2 i_2 + \cdots + a_m i_m \equiv b \bmod d_1\}.$$

For any point $(i_1, \dots, i_m) \in \mathbb{Z}^m$ we have $(i_1, \dots, i_m) \in I$ if and only if $(i_2, \dots, i_m) \in I'$ and

$$a' i_1 \equiv (b - a_2 i_2 - \cdots - a_m i_m)/d_1 \bmod d' \quad \text{with } 1 \le i_1 \le N. \tag{61}$$

By the preceding considerations (case $m = 1$), for fixed $(i_2, \dots, i_m) \in I'$ the set of solutions i_1 of (61) has cardinality $N/d' + E(i_2, \dots, i_m)$ with

$|E(i_2,\dots,i_m)| \le 1$. From this we deduce that

$$|I| = \sum_{(i_2,\dots,i_m)\in I'} \left(\frac{N}{d'} + E(i_2,\dots,i_m)\right) = \frac{N}{d'}\,|I'| + E' \quad \text{with } |E'| \le |I'|.$$

Since $\gcd(a_2,\dots,a_m,d_1) = 1$, we can also assume by induction that $|I'| = N^{m-1}/d_1 + E''$ with $|E''| \le (3N)^{m-2}$. Combining these estimates gives $|I| = N^m/d + E$ with

$$|E| \le |I'| + N|E''| \le N^{m-1} + (N+1)(3N)^{m-2} \le (3N)^{m-1}. \ \blacksquare$$

The main estimate is the following.

LEMMA A.2. *Let $m, D, N \in \mathbb{N}^*$, and let $a_1,\dots,a_m \in \mathbb{Z}$ be integers with $\gcd(a_1,\dots,a_m,D) = 1$. Then, the set*

$$I = \{(i_1,\dots,i_m) \in \mathbb{Z}^m\,;1 \le i_1,\dots,i_m \le N,\ \gcd(a_1i_1+\cdots+a_mi_m, D) = 1\}$$

has cardinality

$$|I| = N^m \prod_{p\mid D}\left(1-\frac{1}{p}\right) + E \quad \textit{with } |E| \le 2^{\omega(D)}(3N)^{m-1},$$

where the product runs over all prime factors p of D and where $\omega(D)$ stands for the number of distinct prime factors of D.

Proof. For each positive divisor d of D, define

$$I_d = \{(i_1,\dots,i_m) \in \mathbb{Z}^m\,;1 \le i_1,\dots,i_m \le N \text{ and } d \,|\, a_1i_1+\cdots+a_mi_m\}.$$

Since $\gcd(a_1,\dots,a_m,d) = 1$, the preceding lemma gives $|I_d| = N^m/d + E_d$ with $|E_d| \le (3N)^{m-1}$. In terms of the Möbius function μ, the inclusion-exclusion principle gives

$$|I| = \sum_{d\mid D} \mu(d)|I_d|.$$

The conclusion then follows from $\sum_{d\mid D}\mu(d)d^{-1} = \prod_{p\mid D}(1-p^{-1})$ and the fact that D admits exactly $2^{\omega(D)}$ square-free positive divisors. $\blacksquare$

In the present paper, we use the estimate of the above lemma in the following form.

LEMMA A.3. *Let the notation be as in Lemma* A.2, *and let ε and κ be positive real numbers such that $D \le N^\kappa$. If N is sufficiently large in terms of ε, κ and m, then the set I has cardinality at least $N^{m-\varepsilon}$.*

Proof. By Lemma A.2, we have $|I| \ge N^m 2^{-\omega(D)} - 2^{\omega(D)}(3N)^{m-1}$. Since $2^{\omega(D)} = \mathcal{O}(D^\delta)$ for any fixed $\delta > 0$ (see [4, Thm. 315]), we also find that $2^{\omega(D)} \le 2^{\omega(D)}3^{m-1} \le (1/2)N^\varepsilon$ if N is sufficiently large in terms of ε, κ and m. As we may assume that $\varepsilon \le 1/2$, this gives $|I| \ge 2N^{m-\varepsilon} - (1/2)N^{m-1+\varepsilon} \ge N^{m-\varepsilon}$. $\blacksquare$

References

[1] W. D. Brownawell, *Sequences of Diophantine approximations*, J. Number Theory 6 (1974), 11–21.
[2] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Amer. Math. Soc., 1951.
[3] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Probab. Math. Statist. 17, Academic Press, 1974.
[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, 1979.
[5] M. Laurent and D. Roy, *Criteria of algebraic independence with multiplicities and interpolation determinants*, Trans. Amer. Math. Soc. 351 (1999), 1845–1870.
[6] D. Roy, *An arithmetic criterion for the values of the exponential function*, Acta Arith. 97 (2001), 183–194.
[7] —, *Small value estimates for the additive group*, Int. J. Number Theory, to appear; arXiv:0708.2307v1 [math.NT].
[8] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Math. 785, Springer, 1980.
[9] M. Waldschmidt, *Solution du huitième problème de Schneider*, J. Number Theory 5 (1973), 191–202.

Département de Mathématiques
Université d'Ottawa
585 King Edward
Ottawa, Ontario, Canada K1N 6N5
E-mail: droy@uottawa.ca

Received on 30.5.2008 (5725)