Riv. Mat. Univ. Parma, Vol. **13** (2022), 19-29

Francesco Amoroso and Sinnou David

On the Galois group of lacunary polynomials

A Roberto, con affetto. Francesco

Abstract. We show that the Galois group defined by the roots of a lacunary polynomial is large in the sense that it grows faster than polynomially with the degree. Lacunary polynomials are the standard way of producing examples of algebraic numbers with small Weil height. One of the key tools in our proof is a *relative* lower bound by Delsinne for the height of a point in a power of the multiplicative group.

Keywords. Lehmer problem, heights, Galois groups, lacunary polynomials.

Mathematics Subject Classification: 11G50, 11R06, 11R09, 11R27.

1 - Introduction

Given a "generic polynomial" with integer coefficients, we expect that it is irreducible, and moreover with a large Galois group. A concrete instance of this principle is a conjecture of Odlyzko and Poonen [**13**] concerning polynomials with 0, 1 coefficients, recently proved by Breuillard and Varjú [**6**] under RH (see also [**4**] for an unconditional result).

In this article we deal on the contrary with a class of interest of "special" polynomials, namely irreducible lacunary polynomials (also called fewnomials) and we prove that, under some natural assumptions, the size of their Galois group grows more than polynomially in the degree.

Received: May 3, 2021; accepted in revised form: September 14, 2021.

Theorem 1.1. *Let $k \geq 1$ be a fixed integer, $\gamma_1, \ldots, \gamma_k$ non-zero integers and $m_0, \ldots, m_k$ coprime integers with $d := m_0 > \cdots > m_k = 0$. We consider the k-nomial* *

$$X^{m_0} + \gamma_1 X^{m_1} + \cdots + \gamma_{k-1} X^{m_{k-1}} + \gamma_k \in \mathbb{Z}[X]$$

of degree d, which we assume irreducible and not cyclotomic. Let D_{ab} be the degree of its Galois group over $\mathbb{Q}^{\mathrm{ab}}$. Then there exists a function $f_{k,\gamma}(t)$, explicitly depending only on $\gamma_1, \ldots, \gamma_k$, and which grows to infinity with t, such that

$$D_{\mathrm{ab}} \geq d^{f_{k,\gamma}(d)} \ .$$

We can even be a little more precise. Let, in the notations of the theorem, $h^* := k(\max(|\gamma_1|, \ldots, |\gamma_k|) + \log k)$. Then there exists an effective absolute constant $c > 0$ such that

$$D_{\mathrm{ab}} \geq (d/h^*)^{c \log\log(d/h^*)^{1/3}} \ ,$$

provided that $d \geq c^{-1} h^*$.

Note that the degree d of a cyclotomic k-nomial with coprime exponents satisfies $d \leq \exp(Ck)$ for some absolute constant $C > 1$ (see Remark 3.4) and thus it is bounded (for fixed k).

Remark that the assumptions on the irreducibility of the polynomial and on the coprimality of $m_0, \ldots, m_k$ are both needed, as the following two examples show:

$$(X-2)(X^{d-1}-2), \qquad X^d - 2 \ .$$

In both cases the degree of the Galois closure is $\leq d^2$.

The main ingredient in our proof is a lower bound (Proposition 2.4) for the height of an algebraic number α, depending on the size of the Galois group of the normal closure of $\mathbb{Q}^{\mathrm{ab}}(\alpha)/\mathbb{Q}^{\mathrm{ab}}$, and under a Kummerian assumption. To deduce Theorem 1.1 from it, we use the fact that "*roots of lacunary polynomials have small height*".

The proof of Proposition 2.4 is an explicit generalisation of a result of [**1**] where we gave a positive answer to Lehmer's problem (see below) when the degree of the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ grows at most polynomially in the degree of $\mathbb{Q}(\alpha)/\mathbb{Q}$. The main new ingredient in the proof of Proposition 2.4 is a lower bound for multiplicatively independent algebraic numbers of Delsinne [**8**], valid over abelian extensions. This result has a long history, as we briefly recall here.

---

*By convention, a k-nomial will thus be a polynomial with $k+1$ non zero coefficients.

Let α be a non zero algebraic number of degree d, with algebraic conjugates $\alpha_1, \dots, \alpha_d$. Let a be the leading coefficient of a minimal equation of α over $\mathbb{Z}$. As usual we denote by $M(\alpha)$ its Mahler measure

$$M(\alpha) = \log|a| \prod_i \max\{|\alpha_i|, 1\}$$

and by $h(\alpha) = \frac{1}{d} \log M(\alpha)$ its absolute logarithmic Weil height. It is well known (Kronecker) that $h(\alpha) = 0$ if and only if α is a root of unity, which we will exclude from now on. In 1993, Lehmer asks whether there is a positive constant c such that

$$h(\alpha) \geq cd^{-1}.$$

Lehmer's problem is still unsolved, but a celebrated result of Dobrowolski [**9**] implies that for any $\varepsilon > 0$ there is $c(\varepsilon) > 0$ such that $h(\alpha) \geq c(\varepsilon) d^{-1-\varepsilon}$.

In 1999, the authors of the present paper proved in [**1**] a deep generalisation of Dobrowolski's lower bound to multiplicatively independent algebraic numbers. Soon after, in [**2**], Dvornicich and the first author discovered that the height on abelian extensions (of course outside zero and roots of unities) can be bounded from below by a positive *absolute* constant, which is of course much stronger than what Lehmer's conjecture predicts. This suggests to take the field of abelian numbers as the ground field for lower bound for the height (a so called "relative" result). Dobrowolski's lower bound was generalised in this direction in [**3**] by Zannier and the first author. Finally, Delsinne in his Ph.D. Thesis succeed, in a veritable *tour de force*, to merge together the ideas of these three papers.

The present paper is organised as follows. We first prove, in Section 2 a strong lower bound for the height of algebraic numbers in a small Galois extension (this is done by applying Delsinne's result to generators of the Galois module defined by our given algebraic number α) and move in Section 3 towards our intended goal of tackling the Galois groups of roots of lacunary polynomials. After an initial preparation (identifying Kummerian obstruction over the maximal abelian extension), we move on to the proof of the main result.

2 - Lower bound for the height and Galois groups

As explained in the introduction we shall need the "relative" version of Delsinne [**8**]. A simplified version of [**8**, Theorem 1.6] asserts:

Theorem 2.1. *Let $\alpha_1, \dots, \alpha_n$ be multiplicatively independent algebraic numbers. Let $D_{\text{ab}} = [\mathbb{Q}^{\text{ab}}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}^{\text{ab}}]$. Then*

$$h(\alpha_1) \cdots h(\alpha_n) \geq c_2(n)^{-1} D_{\text{ab}}^{-1} \log(16 D_{\text{ab}})^{-\kappa_2(n)}$$

where

$$c_2(n) = \left(2n^2\right)^n \exp\left(64n^2 n!\left(2(n+1)^2(n+1)!\right)^{2n}\right)$$

and

$$\kappa_2(n) = 3n\left(2(n+1)^2(n+1)!\right)^n \ .$$

The above value of $\kappa_2(n)$ appears at [**8**, page 983], just before the statement of Theorem 1.6. The value of $c_2(n)$ is at the beginning of page 984.

We shall apply this lower bound for the height taking for $\alpha_1, \dots, \alpha_n$ to be some of the conjugates of an algebraic number α, so that $h(\alpha_1) = \dots = h(\alpha_n) = h(\alpha)$. This forces, if the height of α is small enough and n is large enough, $D_{\rm ab}$ to be large, as desired. The explicit nature of the lower bound in Theorem 2.1 will allow us to let the dimension n of the ambient space (*slowly*) grow with the degree.

We now introduce some notations which we keep in the sequel of this article.

Notation. *Let α be a non zero algebraic number of degree d over $\mathbb{Q}$, and $\alpha_1, \dots, \alpha_d$ its conjugates over $\mathbb{Q}$. We denote by $\mathcal{M}_\alpha$ the multiplicative group generated by $\alpha_1, \dots, \alpha_d$, by $r(\alpha) := \dim_{\mathbb{Q}}(\mathcal{M}_\alpha \otimes_{\mathbb{Z}} \mathbb{Q})$ its rank and by $e(\alpha)$ the exponent of its torsion subgroup.*

The following lemma is implicit in the proof of [**1**, Corollaire 6.1, p.177].

Lemma 2.2. *Let α be a non zero algebraic number, and assume $r = r(\alpha) \geq 1$. Then the degree D' of the normal closure of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$ satisfies $D' \leq 3^{r^2}$.*

Proof. Let $e = e(\alpha)$ and G be the Galois group of $\mathbb{Q}(\alpha_1^e, \dots, \alpha_d^e)/\mathbb{Q}$. Note that as $\mathbb{Z}$-module of finite type, $\mathcal{M}_\alpha = F \oplus T$, where T is a torsion and F is free; by definition of e, the kernel of the multiplication $[e] : \mathcal{M}_\alpha \longrightarrow \mathcal{M}$ $x \longmapsto x^e$ is T and thus $\mathcal{M}_{\alpha^e} = [e]\mathcal{M}_{\alpha^e}$ is torsion free. Hence, the action of G over $\mathcal{M}_{\alpha^e}$ defines an injective representation $G \to {\rm GL}_r(\mathbb{Z})$. Thus, G identifies to a finite subgroup of ${\rm GL}_r(\mathbb{Z})$. To conclude we can now use a theorem of Minkowski [**14**, page 197] which asserts that the reduction mod 3 from ${\rm GL}_r(\mathbb{Z})$ to ${\rm GL}_r(\mathbb{Z}/3\mathbb{Z})$ is injective on finite subgroups of ${\rm GL}_r(\mathbb{Z})$, see also [**15**]. □

Remark 2.3. *Even if it is not necessary for our purposes, we note that much better results hold. Feit*[†] *([**10**]) shows that the group of signed permutation matrices (the group of $r \times r$ matrices with entries in $\{-1, 0, 1\}$ having exactly one nonzero entry in each row and each column) has maximal order ($= 2^r r!$) for $r =$*

[†] As pointed out by G. Rémond, the table in [**10**] contains an error which stands corrected in [**5**], Table 2.

$1, 3, 5$ *and for* $r > 10$. *For the seven remaining values of* r, *Feit characterizes the corresponding maximal groups, showing that the maximal order is* $\epsilon(r) \cdot 2^r r!$ *with* $\epsilon(r)$ *explicit. See* [**11**] *for more details and for a proof of the weaker statement* $n(r) \le 2^r r!$ *for large* r.

We can now state and prove the main result of this section.

Proposition 2.4. *Let* α *be a non zero algebraic number which is not a root of unity. Let us assume*

$$\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)}) = \mathbb{Q}^{\mathrm{ab}}(\alpha) \ .$$

Then,

$$h(\alpha) \ge (16D_{\mathrm{ab}})^{-C \log\log(16D_{\mathrm{ab}})^{-1/3}} \ ,$$

where D_{ab} *is the degree of the normal closure of* $\mathbb{Q}^{\mathrm{ab}}(\alpha)/\mathbb{Q}^{\mathrm{ab}}$ *and* $C \ge 1$ *is an effective absolute constant.*

Proof. The strategy of the proof is the following. Lemma 2.2 forces the multiplicative rank of the galois modules $\mathcal{M}(\alpha)$ to be large enough, thus providing enough *multiplicatively independent* conjugates of α, say $\alpha_1, \dots, \alpha_r$ which all lie by definition in the normal closure of $\mathbb{Q}(\alpha)$. One can then make use of the Theorem 2.1. The caveat is that the dependence in the number of algebraic numbers considered in this result is very weak and thus, one needs a very slowly growing functions.

We first remark that if D_{ab} is bounded, our result easily follows by any "relative" lower bound of the shape

$$h(\alpha) \ge f([\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}])$$

with $f\colon \mathbb{N} \to \mathbb{R}^+$ since α is not a root of unity. For instance, the main result of [**3**] is largely enough. Thus we freely assume D_{ab} sufficiently large[‡] to ensure that all the displayed inequalities hold.

Let

$$x := \log\log(16D_{\mathrm{ab}})^{1/3} \quad \text{and} \quad n := [x] - 2.$$

We claim that:

Fact. $n \le r := r(\alpha)$.

[‡]Note that this in particular ensures that α is not a root of unity since otherwise D_{ab} would be equal to 1.

Proof. Indeed, let D' and D'_{ab} be respectively the degree of the normal closure of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$ and of $\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})/\mathbb{Q}^{\mathrm{ab}}$. By assumption $D'_{\mathrm{ab}} = D_{\mathrm{ab}}$. Since $D' \geq D'_{\mathrm{ab}}$, by Lemma 2.2 we have $D_{\mathrm{ab}} \leq D' \leq 3^{r^2}$ and

$$(n+2)\log(n+2) \leq x\log x \leq \log\log(27D_{\mathrm{ab}}) \leq \log((r^2+3)\log 3)\ .$$

An elementary computation shows that $\log((r^2+3)\log 3) \leq (r+2)\log(r+2)$, thus $n \leq r$ as required. □

By the Fact above, there exist at least n multiplicatively independent conjugates of α, say $\alpha_1, \dots, \alpha_n$. Theorem 2.1 shows that $h(\alpha) \geq e^{-U}$ where

$$U = \frac{1}{n}\log D_{\mathrm{ab}} + \frac{1}{n}\log(c_2(n)) + \frac{\kappa_2(n)}{n}\log\log(16D_{\mathrm{ab}})$$

and with $c_2(n)$ and $\kappa_2(n)$ defined in that theorem. An elementary computation shows that

$$(2.1)\qquad \begin{cases} \dfrac{1}{n}\log(c_2(n)) = \log(2n^2) + 64n\cdot n!\left(2(n+1)^2(n+1)!\right)^{2n} \leq cn^{2n^2} \\[2ex] \qquad\qquad \dfrac{\kappa_2(n)}{n} = 3\left(2(n+1)^2(n+1)!\right)^{n} \leq cn^{2n^2} \end{cases}$$

for some $c \geq 1$ (and indeed we may take $c = 1$). Thus, taking into account $n \leq x$ and $n \geq x - 2 \geq \frac{x}{2}$,

$$U \leq \left(\frac{1}{n} + \frac{2cn^{2n^2}\log\log(16D_{\mathrm{ab}})}{\log(16D_{\mathrm{ab}})}\right)\log(16D_{\mathrm{ab}})$$
$$\leq \frac{4c}{x}\max\left\{1, x^{3x^2}\log(16D_{\mathrm{ab}})^{-1/2}\right\}\log(16D_{\mathrm{ab}})\ .$$

We remark that

$$3x^2\log x \leq \log\log(16D_{\mathrm{ab}})^{2/3}\log\log\log(16D_{\mathrm{ab}}) \leq \frac{1}{2}\log\log(16D_{\mathrm{ab}})\ .$$

Thus $x^{3x^2} \leq \log(16D_{\mathrm{ab}})^{1/2}$ and

$$U \leq \frac{4c}{x}\log(16D_{\mathrm{ab}}) = 4c\log\log(16D_{\mathrm{ab}})^{-1/3}\log(16D_{\mathrm{ab}})\ .$$

□

Remark 2.5.

1. *We could replace in the statement of the last proposition* $C\log\log(16D_{\text{ab}})^{-1/3}$ *by* $C\log\log(16D_{\text{ab}})^{-1/2+\varepsilon}$ *and even by* $C\log\log(16D_{\text{ab}})^{-1/2}\log\log\log(16D_{\text{ab}})$ *at the cost of more involved computations. Also the values of the various* C *can be made explicit, again after several annoying computations.*

2. *Perhaps more interesting, the reader could remark that the inequality* $r \geq n$ *in the* Fact *is far from being optimal: we can indeed ensure that* $r \geq n^{\varepsilon n}$ *for a sufficiently small* ε. *However having more multiplicatively independent conjugates does not improve the final result, due to the dependence* (2.1) *in the dimension of Delsinne's lower bound.*

3. *It is worthwile noting that the hypothesis* $D'_{\text{ab}} = D_{\text{ab}}$ *(in other words, that there is no Kummerian obstruction) is a simplifying hypothesis. One can easily prove, with the same argument, a general result taking into account the precise value of the exponent of the torsion subgroup of* $\mathcal{M}_\alpha$. *Again, this would only come at the cost of elementary but cumbersome computations.*

3 - Size of the Galois group of a lacunary polynomial

In this section, we prove a general result on the size of the Galois group of a root of a lacunary polynomial, and we deduce Theorem 1.1 from it.

To start with, we first remark that the assumption $\mathbb{Q}^{\text{ab}}(\alpha^{e(\alpha)}) = \mathbb{Q}^{\text{ab}}(\alpha)$ of Proposition 2.4 is easily read on the minimal polynomial of α over $\mathbb{Q}$. Indeed, one has the easy:

Lemma 3.1. *Let* α *be an algebraic number with minimal polynomial* $P(X)$ *over* $\mathbb{Q}$. *Let us consider the following assertion:*

1) P *is not a polynomial in* X^δ *for* δ *integer* > 1.

2) *For any integer* $e \geq 1$ *we have* $\mathbb{Q}^{\text{ab}}(\alpha^e) = \mathbb{Q}^{\text{ab}}(\alpha)$.

Then 1) *implies* 2).[§]

Proof. Let $e \geq 1$ and $E := \mathbb{Q}^{\text{ab}}(\alpha^e) \cap \mathbb{Q}(\alpha)$. We note $\delta = [\mathbb{Q}(\alpha) : E]$ and $\alpha' = \text{Norm}_E^{\mathbb{Q}(\alpha)}(\alpha) \in E$. The algebraic conjugates of α over E are multiples of α by a root of unity. Thus $\alpha' = \zeta\alpha^\delta$ for some root of unity ζ. Since $\zeta = \alpha'/\alpha^\delta \in \mathbb{Q}(\alpha)$ we have $\zeta \in \mathbb{Q}^{\text{ab}} \cap \mathbb{Q}(\alpha) \subseteq E$ and thus also $\alpha^\delta \in E$. Let

$$Q(X) = \prod_{\substack{\sigma\colon E \hookrightarrow \overline{\mathbb{Q}} \\ \sigma_{|\mathbb{Q}} = \text{Id}}} (X^\delta - \sigma\alpha^\delta) \in \mathbb{Q}[X] \ .$$

[§]Note that 2) does not imply 1), as we can see taking $\alpha = \sqrt{2} \in \mathbb{Q}^{\text{ab}}$.

Then $Q(\alpha) = 0$ and $\deg Q = \delta \times [E : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Thus $Q = P$. Since Q is a polynomial in X^δ, by assumption we have $\delta = 1$, *i. e.* $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}^{\mathrm{ab}}(\alpha^e)$. This implies $\mathbb{Q}^{\mathrm{ab}}(\alpha^e) = \mathbb{Q}^{\mathrm{ab}}(\alpha)$ as claimed. □

We also need to show that the number of non zero coefficients of a cyclotomic polynomial of square free order grows to infinity. We have not found a standard reference for this result, thus we reproduce here an answer given by G. Kós to a question posed on the web site *math.stackexchange*, see [**12**].

Lemma 3.2. *Let ϕ_n be a cyclotomic polynomial of order n and let p be a prime such that $p \mid n$ and $p^2 \nmid n$. Then ϕ_n has at least p non zero coefficients.*

Proof. We argue by contradiction, assuming $\phi_n(x) = \sum_{i=1}^{p-1} a_i x^{m_i}$ for some integers a_i, m_i with $m_i \geq 0$. Using the box principle, we select an integer u such that none of $m_1 + u, \ldots, m_{p-1} + u$ is divisible by p. Let $r = n/p$, $\omega = e^{2\pi i/n}$ and consider the sum

$$S := \sum_{j=1}^{p} \omega^{jru} \phi_n(\omega^{jr+1}).$$

Since $p \nmid r$, among the numbers $\omega^{r+1}, \ldots, \omega^{pr+1}$ there are precisely $p - 1$ primitive nth root of unity and a root of unity of order r. Thus $S \neq 0$. On the other hand

$$S = \sum_{j=1}^{p} \omega^{jru} \sum_{i=1}^{p-1} a_i \omega^{(jr+1)m_i} = \sum_{i=1}^{p-1} a_i \omega^{m_i} \sum_{j=1}^{p} \omega^{jr(m_i+u)}.$$

Now ω^r is a primitive pth root of unity, thus $\sum_{j=1}^{p} \omega^{jrk} = 0$ for any integer k not divisible by p. Since, by our choice of u, none of the $m_i + u$ is divisible by p, we conclude that $S = 0$, a contradiction. □

We can now state and prove our result on the size of the Galois group of a root of a lacunary polynomial.

Proposition 3.3. *Let $\gamma_0, \gamma_1, \ldots \gamma_k \in \overline{\mathbb{Q}}^*$ and $m_0, \ldots, m_k \in \mathbb{Z}$ with $0 = m_k < m_{k-1} < \cdots < m_1 < m_0 =: d$. We set $h^* := k(h(\boldsymbol{\gamma}) + \log k)$, where $h(\boldsymbol{\gamma})$ is the Weil height of the projective point $(\gamma_0 : \cdots : \gamma_k)$. Let α be a root of*

$$\gamma_0 X^{m_0} + \gamma_1 X^{m_1} + \cdots + \gamma_{k-1} X^{m_{k-1}} + \gamma_k = 0 \ .$$

We assume:

1. *there is no $l < k$ such that the subsum $\gamma_0 \alpha^{m_0} + \cdots + \gamma_l \alpha_l^{m_l}$ vanishes,*

2. *α is not a root of unity,*

3. $\mathbb{Q}^{\mathrm{ab}}(\alpha) = \mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})$.

Then there exists an effective absolute constant $c > 0$ such that, if $d \geq c^{-1}h^*$, the degree D_{ab} of the Galois closure of $\mathbb{Q}^{\mathrm{ab}}(\alpha)/\mathbb{Q}^{\mathrm{ab}}$ satisfies

$$D_{\mathrm{ab}} \geq (d/h^*)^{c \log\log(d/h^*)^{1/3}} .$$

Proof. By the assumption 1. on non-vanishing subsums, we can apply [**7**, Lemma 2.2] to get

$$(m_l - m_{l+1})h(\alpha) \leq h(\boldsymbol{\gamma}) + \log\max\{l+1, k-l\}$$

for $l = 0, \dots, k-1$. Summing over l we obtain $dh(\alpha) \leq k(h(\boldsymbol{\gamma}) + \log k) = h^*$. Thus we have the upper bound

$$h(\alpha) \leq \exp(-\log(d/h^*)) .$$

By assumptions 2. and 3., we can apply Proposition 2.4 to get the lower bound

$$h(\alpha) \geq (16D_{\mathrm{ab}})^{-C\log\log(16D_{\mathrm{ab}})^{-1/3}} .$$

Comparing the two bounds, we get

$$\log(d/h^*) \leq C \log\log(16D_{\mathrm{ab}})^{-1/3} \log(16D_{\mathrm{ab}})$$

which easily implies

$$\log(D_{\mathrm{ab}}) \geq c \log\log(d/h^*)^{1/3} \log(d/h^*)$$

for some $c > 0$, provided that $d/h^* \geq c^{-1}$. □

Proof of Theorem 1.1. We fix a positive integer k and non zero integers $\gamma_1, \dots, \gamma_k \in \mathbb{Z}$. Let $m_0, \dots, m_k \in \mathbb{Z}$ coprime with $0 = m_k < \cdots < m_0$ and with $d := m_0$ sufficiently large with respect to k and $\gamma_1, \dots, \gamma_k$. We consider the polynomial

$$P_{\mathbf{m}} = X^{m_0} + \gamma_1 X^{m_1} + \cdots + \gamma_{k-1}X^{m_{k-1}} + \gamma_k \in \mathbb{Z}[X]$$

which we assume irreducible and not cyclotomic. Let α be a root of $P_{\mathbf{m}}$. Since $P_{\mathbf{m}}$ is irreducible, there is no vanishing subsum of the form $\alpha^{m_0} + \gamma_1\alpha^{m_1} + \cdots + \gamma_l\alpha_l^{m_l}$ with $l < k$.

Since our polynomial is not cyclotomic, α is not a root of unity. Moreover, since $m_0, \dots, m_k$ are coprime, $P_{\mathbf{m}}$ is not a polynomial in X^δ for $\delta > 1$. By Lemma 3.1, $\mathbb{Q}^{\mathrm{ab}}(\alpha) = \mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})$. All the assumptions of Proposition 3.3 are now satisfied and we get

$$D_{\mathrm{ab}} \geq (d/h^*)^{c \log\log(d/h^*)^{1/3}}$$

provided that $d/h^* \geq c^{-1}$. □

Remark 3.4. *Let, as in the theorem, $k \geq 1$ be a fixed integer, $\gamma_1, \dots, \gamma_k$ non-zero integers, and $m_0, \dots, m_k$ coprime integers with $d := m_0 > \cdots > m_k = 0$. If $P_{\mathbf{m}} := X^{m_0} + \gamma_1 X^{m_1} + \cdots + \gamma_{k-1} X^{m_{k-1}} + \gamma_k$ is cyclotomic of order, say, n, then n is squarefree since the exponents are coprime by assumption*¶. *Let p be the largest prime divisor of n; using a standard upper bound for the first Čebyšëv function $\theta(x) = \sum_{p \leq x} \log(p)$, one derives $\log d \leq \log n \leq Cp$ for some absolute constant $C > 1$. By Lemma 3.2, $k \geq p$. Thus $d \leq \exp(Ck)$.*

Acknowledgments. We sincerely thank the referee of the present article for significant and precise comments, helping us to improve the exposition in various aspects.

References

[**1**] F. Amoroso and S. David, *Le problème de Lehmer en dimension supérieure,* J. Reine Angew. Math. **513** (1999), 145–179.

[**2**] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions,* J. Number Theory **80** (2000), 260–272.

[**3**] F. Amoroso and U. Zannier, *A relative Dobrowolski lower bound over abelian extensions,* Ann. Scuola Norm. Sup. Pisa Cl. Sci. **29** (2000), 711–727.

[**4**] L. Bary-Soroker and G. Kozma, *Irreducible polynomials of bounded height,* Duke Math. J. **169** (2020), 579–598.

[**5**] N. Berry, A. Dubickas, N. D. Elkies, B. Poonen and C. Smyth, *The conjugate dimension of algebraic numbers,* Q. J. Math. **55** (2004), 237–252.

[**6**] E. Breuillard and P. P. Varjú, *Irreducibility of random polynomials of large degree,* Acta Math. **223** (2019), 195–249.

[**7**] P. Corvaja and U. Zannier, *On the rank of certain matrices,* Math. Nachr. **284** (2011), 1652–1657.

¶and since $\phi_{p^r m}(x) = \phi_{pm}(x^{p^{r-1}})$ for p prime, $p \nmid m$.

[**8**] E. Delsinne, *Le problème de Lehmer relatif en dimension supérieure,* Ann. Sci. Éc. Norm. Supér. **42** (2009), 981–1028.

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

[**10**] W. Feit, *Orders of finite linear groups,* Proc. First Jamaican Conference on Group Theory and its Applications (Kingston, 1996), Univ. West Indies, Kingston, 1996, 9–11.

[**11**] S. Friedland, *The maximal orders of finite subgroups in* $\mathrm{GL}_n(\mathbb{Q})$*,* Proc. Amer. Math. Soc. **125** (1997), 3519–3526.

[**12**] G. Kós, *A cyclotomic polynomial whose index has a large prime divisor cannot be too sparse,* Mathematics Stack Exchange, https://math.stackexchange.com/q/988963.

[**13**] A. M. Odlyzko and B. Poonen, *Zeros of polynomials with 0,1 coefficients,* Enseign. Math. **39** (1993), 317–348.

[**14**] H. Minkowski, *Zur Theorie der positiven quadratischen Formen,* J. Reine Angew Math. **101** (1887), 196–202.

[**15**] J.-P. Serre, *Rigidité du foncteur de Jacobi d'échelon* $n \geq 3$*,* Appendice à l'exposé 17 du Séminaire Cartan, 1960/1961.

Francesco Amoroso
Laboratoire de mathématiques Nicolas Oresme,
CNRS UMR 6139
Normandie Université, Université de Caen,
Campus II, BP 5186, 14032 Caen Cedex, France
e-mail: francesco.amoroso@unicaen.fr

Sinnou David
Institut de Mathématiques de Jussieu-Paris Rive Gauche
CNRS UMR 7586
Sorbonne Université,
4, place Jussieu, 75005 Paris, France
&
CNRS UMI 2000 Relax
Institute of Mathematical Sciences,
IV Cross Road, CIT Campus Taramani
Chennai 600 113, Tamil Nadu, India
e-mail: sinnou.david@imj-prg.fr