Lehmer's problem for small Galois groups

Francesco Amoroso

LEHMER'S PROBLEM FOR SMALL GALOIS GROUPS

F. AMOROSO

1. Introduction

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 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 [8] implies that for any $\varepsilon > 0$ there is $c(\varepsilon) > 0$ such that $h(\alpha) \geq c(\varepsilon) d^{-1-\varepsilon}$. More precisely he shows that

$$h(\alpha) \geq \frac{c}{d} \left(\frac{\log(3d)}{\log\log(3d)} \right)^{-3}$$

with $c > 0$ absolute constant.

Let $D := [\mathbb{Q}(\alpha_1, \dots, \alpha_d) : \mathbb{Q}]$ be the degree of the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$. More recently, David with the author gave a positive answer to Lehmer's problem when D growth at most polynomially in d. More precisely,

Theorem 1.1 ([1], *Corollaire* 1.7)**.** *Let m be a fixed positive integer. Then there exists $c(m) > 0$ such that*

$$h(\alpha) \geq c(m) d^{-1}$$

provided that

$$D \leq d^m. \tag{1.1}$$

One could ask if it is possible to relax condition (1.1): does there exist a real function $t \mapsto f(t)$ with $\lim_{t \mapsto +\infty} f(t) = \infty$ and a constant $c > 0$ such that $h(\alpha) \geq cd^{-1}$ provided that $D \leq d^{f(d)}$?

As pointed out by Bardestani [5] (see Proposition 2.1) this question is logically equivalent to a positive answer to the full Lehmer's problem, and thus it seems beyond the state of the art. Nevertheless, the proof of Proposition 2.1 suggests that the obstruction to relax condition (1.1) is related to the existence of a small degree subextension $\mathbb{Q}(\alpha^e)/\mathbb{Q}$ of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

As a special case of a more general result (Theorem 5.1) we prove the following generalization of Theorem 1.1:

Date: February 20, 2020.

Theorem 1.2. *Let α be a non zero algebraic number of degree d, let D be the degree of the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$. We also let*

$$d_0 = \min_{e\geq 1}[\mathbb{Q}(\alpha^e):\mathbb{Q}]$$

and we assume

$$D \leq \frac{1}{4} d^{500^{-1}\log(\rho d_0)^{1/6}}$$

for some $\rho \geq 16$. Then, if α is not a root of unity,

$$h(\alpha) \geq \frac{1}{\rho d}.$$

Theorem 1.2 is a consequence of Theorem 3.1 which provides a lower bound for the height depending on the size of two Galois groups. Theorem 3.1, combined with the fact that "roots of lacunary polynomials have small height", also applies to show that the size of the Galois group of a lacunary polynomial growths more than polynomially in the degree, under some natural assumptions.

Theorem 1.3. *Let $\gamma_1, \dots, \gamma_k$ non-zero integers and $0 = m_k < \cdots < m_0 = d$ coprime integers. We consider the polynomial*

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

of degree d, which we assume irreducible. Let D_{ab} be the degree of its Galois closure over $\mathbb{Q}^{\mathrm{ab}}$. Then there exists a function $f(t)$ explicitly depending on $|\boldsymbol{\gamma}| := \max(|\gamma_1|, \dots, |\gamma_k|)$ and which growth to infinity with t, such that

$$D_{\mathrm{ab}} \geq d^{f(d)}.$$

More precisely, let $h^* := k(|\boldsymbol{\gamma}| + \log k)$. Then, if $d \geq 16h^*$,

$$D_{\mathrm{ab}} \geq \frac{1}{16}(d/h^*)^{10^{-7}(\log\log(d/h^*))^{1/4}}.$$

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

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

The new ingredients in the proofs of our results are two explicit versions of the main theorem of [1]. The first one provides a good dependence in the dimension n of the ambient space:

Theorem 1.4 ([3], Corollary 1.6)**.** *Let $\alpha_1, \dots, \alpha_n$ be multiplicatively independent algebraic numbers in a number field. Let $D = [\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}]$. Then*

$$h(\alpha_1)\cdots h(\alpha_n) \geq D^{-1}\big(1050 n^5 \log(3D)\big)^{-n^2(n+1)^2}.$$

The lower bound [1] for the height was previosly extended by Delsinne [7], to prove a so called "relative" result, replacing the degree over $\mathbb{Q}$ by the degree over $\mathbb{Q}^{\mathrm{ab}}$. More precisely, a simplified version of [7, Theorem 1.6] asserts:

Theorem 1.5 ([7], Theorem 1.6)**.** *Let $\alpha_1, \dots, \alpha_n$ be multiplicatively independent algebraic numbers. Let $D_{\mathrm{ab}} = [\mathbb{Q}^{\mathrm{ab}}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}^{\mathrm{ab}}]$. Then*

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

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

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

Roughly speaking, Theorem 1.5 allows to replace D_{ab} by D at the cost of replacing the exponent on the error terms in Theorem 1.4 (which is approximately n^3) by n^{n^2}. It is likely that the method of [3] could be adapted to prove such a relative result with a much better exponent. To have a result depending on the degree over $\mathbb{Q}^{\mathrm{ab}}$ is important in several application, and for instance in the proof of Theorem 1.3 (see Remark 4.2).

We shall apply these lower bounds for the height taking for $\alpha_1, \ldots, \alpha_n$ some of the conjugates of an algebraic number α, so that $h(\alpha_1) = \cdots = h(\alpha_n) = h(\alpha)$. The explicit nature of the lowers bounds in Theorems 1.4 and 1.5 will allow us to let the dimension of the ambient space logarithmically growing with the degree, which was not allowed using the main theorem of [1].

The proofs of our results are not difficult, but the explicit computations are involved, due to the nature of the lower bounds for the height of Theorems 1.4 and 1.5. For the convenience of reader, we begin the proofs of Theorems 3.1 and 5.1 with a short explanation of the strategy.

2. Notations and auxiliary results

We first state and prove the following proposition announced in the introduction.

Proposition 2.1. *Let us assume that there exists a function $d \mapsto f(d)$ with $\lim_{d\mapsto+\infty} f(d) = \infty$ and a constant $c > 0$ such that $h(\alpha) \geq cd^{-1}$ for any non zero algebraic number α which is not a root of unity, provided that the degree D of the normal closure $\mathbb{Q}(\alpha)/\mathbb{Q}$ satisfies $D \leq d^{f(d)}$. Then the same conclusion holds without any assumption on D.*

Proof. Let α' be a non zero algebraic number of degree d' which is not a root of unity. We can find a sequence e_k of positive integers with $\lim_{k\to+\infty} e_k = +\infty$ such that the polynomials $P_k = X^{e_k} - \alpha' \in \mathbb{Q}(\alpha')[X]$ are irreducible. For each k, we select a root $\alpha_k \in \overline{\mathbb{Q}}^*$ of P_k. Thus $[\mathbb{Q}(\alpha_k) : \mathbb{Q}(\alpha')] = e_k$ and $d_k := [\mathbb{Q}(\alpha_k) : \mathbb{Q}] = d'e_k$. We also remark that the degree D_k of the normal closure of $\mathbb{Q}(\alpha_k)/\mathbb{Q}$ is bounded by $D'e_k^{d'}\phi(e_k) \leq D'e_k^{d'+1}$, where D' denotes the degree of the normal closure of $\mathbb{Q}(\alpha')/\mathbb{Q}$. Thus

$$\frac{\log D_k}{\log d_k} \leq \frac{\log D' + (d'+1)\log e_k}{\log d' + \log e_k} \to d' + 1 \text{ as } k \to +\infty.$$

By assumption, $D_k \leq d_k^{f(d_k)}$ for large k. Thus, again by assumption, $h(\alpha_k) \geq \frac{c}{d_k}$ and

$$h(\alpha') = e_k h(\alpha_k) \geq e_k \cdot \frac{c}{d_k} = \frac{c}{d'}.$$

□

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, with algebraic conjugates $\alpha_1, \dots, \alpha_d$. 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 cardinality of its torsion subgroup.*

Lemma 2.2. *Let α be a non zero algebraic number, not a root of unity. Let $r = r(\alpha) \geq 1$. Then the degree D' of the normal closure of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$ satisfies*

$$D' \leq D_{\max}(r) := \epsilon(r) \cdot 2^r r!$$

where

$$\epsilon(2) = \frac{3}{2},\ \epsilon(4) = 3,\ \epsilon(6) = \frac{9}{4},\ \epsilon(7) = \frac{9}{2},\ \epsilon(8) = \frac{135}{2},\ \epsilon(9) = \frac{15}{2}, 15,\ \epsilon(10) = \frac{9}{4}$$

and $\epsilon(r) = 1$ for a positive integer $r \notin \{2, 4, 6, 7, 8, 9, 10\}$.

Proof. (see also the proof of [1, *Corollaire* 6.1] and [4, Theorem 18]). Let $e = e(\alpha)$ and G be the Galois group of $\mathbb{Q}(\alpha_1^e, \dots, \alpha_d^e)/\mathbb{Q}$. Since $\mathcal{M}_{\alpha^e}$ is torsion free, the action of G over $\mathcal{M}_{\alpha^e}$ defines an injective representation $G \to \mathrm{GL}_r(\mathbb{Z})$. Thus G identifies to a finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$. Feit [9] (unpublished) shows that the group of signed permutation group (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 $r = 1, 3, 5$ 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 $\epsilon(r)$ as above. See [10] for more details and for a proof of the weaker statement $n(r) \leq 2^r r!$ for large r.

□

Notation. *For $t > e$ we set*

$$l(t) = \frac{\log(t)}{\log\log(t)}.$$

For $t > e^e$, we also note

$$l_2(t) = l(\log t) = \frac{\log\log(t)}{\log\log\log(t)}.$$

Remark 2.3.

i) The fonction $t \mapsto l(t)$ is decreasing to e on $(e, e^e]$ and increasing on $[e^e, +\infty)$. Thus, for $e < t_0 \leq t_1 < t_2$ we have $l(t_1) \leq e^{-1} l(t_0) l(t_2)$.

ii) We have $\log(t)^{1/2} \leq l(t)$, and, for $t \geq t_0 > e$, $l(t) \leq (\log\log(t_0))^{-1} \log(t)$.

3. Lower bound for the height and Galois groups

This section is devoted to the proof of the following theorem, which provides a lower bound for the height depending on the size of two Galois groups.

Theorem 3.1. *Let α be a non zero algebraic number which is not a root of unity. I) Let D and D' be respectively the degrees of the normal closures of $\mathbb{Q}(\alpha)/\mathbb{Q}$ and of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$. Then, for every $\alpha' \in \mathbb{Q}(\alpha)$ such that $r(\alpha') \geq r(\alpha)$ we have*

$$h(\alpha') \geq e^{-U}$$

with

$$U \le 8 \max\left\{ l(4D)^{-1/4},\ l(4D')^{-1} \right\} \log(4D). \tag{3.1}$$

II) Let D_{ab} and D' be respectively the degrees of the normal closures of $\mathbb{Q}^{\mathrm{ab}}(\alpha)/\mathbb{Q}^{\mathrm{ab}}$ and of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$. Then, for every $\alpha' \in \mathbb{Q}^{\mathrm{ab}}(\alpha)$ such that $r(\alpha') \ge r(\alpha)$ we have

$$h(\alpha') \ge e^{-U}$$

with

$$U \le 72 \cdot 10^3 \max\left\{ l_2(16D_{\mathrm{ab}})^{-1/2},\ l(16D')^{-1} \right\} \log(16D_{\mathrm{ab}}). \tag{3.2}$$

Proof. The strategy of the proof of I) and II) is the following. Lemma 2.2 provides us with a lower bound of $r(\alpha)$ in terms of D', say $r(\alpha) \ge r(D')$. Since $r(\alpha') \ge r(\alpha)$, for any positive integer $n \le r(D')$ there exist n multiplicatively independent conjugates of α', say $\alpha'_1, \dots, \alpha'_n$. Since $h(\alpha'_1) = \cdots = h(\alpha'_n) = h(\alpha')$, the lower bounds for the height (Theorem 1.4 to prove assertion I) and Theorem 1.5 for assertion II) give $h(\alpha') \ge e^{-U}$ where U is an explicit function depending on n and on D (case I) or D_{ab} (case II). We choose $n \le r(D')$ for which U is smaller.

We prove I). By assumption α is not a root of unity, thus $r := r(\alpha) \ge 1$. Since $r(\alpha') \ge r$, in particular α' is not a root of unity.

If $l(4D') \le l(4) \le 9/2$ then $U \ge \frac{16}{9} \log(4D)$. Thus our bound follows from a reasonable lower bound for the height. Indeed, if $D = 1$, then $h(\alpha') \ge \log 2 \ge 4^{-16/9}$ and, if $D \ge 2$,

$$h(\alpha') \ge 2D^{-1} \log(3D)^{-3} \ge (4D)^{-16/9}$$

by [12, Corollary 2]. Thus we assume from now on $l(4D') > l(4) > 4$, which easily implies $D \ge D' \ge 14\,000$.

By Lemma 2.2,

$$D' \le D_{\max}(r)$$

with $D_{\max}(r)$ defined in the statement of the lemma. Since $D' \ge 14\,000$ and $D_{\max}(r) \le 3\,840$ for $r = 2, 3, 4, 5, 6$ we must have $r \ge 7$. Let

$$x := \min\left\{ l(4D)^{1/4},\ l(4D') \right\} \ge 4$$

and $n := [x] - 1 \ge 3$.

We claim that $n \le r$ as we now show. We have $n \le l(4D') - 1$. An easy computation shows that $l(4D') \log l(4D') \le \log D'$. Moreover $D_{\max}(r) = 2^r r! \le r^r$ for $r > 10$. Thus in this range

$$n \log n \le l(4D') \log l(4D') \le \log D' \le r \log r$$

which ensures that $n \le r$, at least if $r > 10$. For $r = 7, 8, 9, 10$, a direct computation shows that again

$$n \le l(4D') - 1 \le l(4D_{\max}(r)) - 1 \le r.$$

By assumption $r \le r(\alpha')$. Thus there exist at least n multiplicatively independent conjugates of α', say $\alpha'_1, \dots, \alpha'_n$. Since $h(\alpha'_1) = \cdots = h(\alpha'_n) = h(\alpha')$, Theorem 1.4 shows that

$$h(\alpha') \ge D^{-1/n} \big(1050 n^5 \log(3D)\big)^{-n(n+1)^2} = e^{-U}$$

with

$$U = \frac{1}{n}\log D + n(n+1)^2 \log\Big(1050 n^5 \log(3D)\Big). \tag{3.3}$$

We have to prove (3.1). Since $D \geq 14\,000$ we have $n \leq l(4D)^{1/4} \leq \log(4D)^{1/4}$ and

$$\begin{aligned}\log\Big(1050 n^5 \log(3D)\Big) &\leq \log(1050) + \frac{5}{4}\log\log(4D) + \log\log(4D)\\ &\leq \left(\frac{\log(1050)}{\log\log(4\cdot 14\,000)} + \frac{9}{4}\right)\log\log(4D) \leq 6\log\log(4D).\end{aligned}$$

By (3.3) and using $n \geq x-2 \geq \frac{x}{2}$ (from $x \geq 4$) and $n(n+1)^2 \leq x^3$ (from $n \leq x-1$) we deduce

$$\begin{aligned}U &\leq \left(\frac{1}{n} + n(n+1)^2 \frac{\log\Big(1050 n^5 \log(3D)\Big)}{\log(4D)}\right)\log(4D)\\ &\leq 8\max\left\{\frac{1}{x}, x^3 l(4D)^{-1}\right\}\log(4D).\end{aligned}$$

Since $x^4 \leq l(4D)$, we finally get

$$U \leq \frac{8}{x}\log(4D) = 8\max\Big\{l(4D)^{-1/4},\ l(4D')^{-1}\Big\}\log(4D).$$

Inequality (3.1) is proved.

We now prove II). We follow the same pattern of the previous proof. We let $r := r(\alpha) \geq 1$.

If $l(16D') \leq 12$ then the R.H.S of (3.2) is $\geq 6\,000\log(16D_{\mathrm{ab}})$ and our lower bound directly follows from Theorem 1.5, taking $n = 1$:

$$h(\alpha') \geq \frac{1}{2}\exp(-16\,384)D_{\mathrm{ab}}^{-1}\log(16D_{\mathrm{ab}})^{-48} \leq (16D_{\mathrm{ab}})^{-6\,000}.$$

We assume from now on $l(16D') > 12$, which easily implies $D \geq D' \geq 10^{19}$.

Let

$$x := \min\left\{\frac{1}{6}l_2(16D_{\mathrm{ab}})^{1/2},\ l(16D')\right\} \geq 12$$

and $n := [x] \geq 12$.

As in the proof of part I), $n \leq r$. Indeed by Lemma 2.2, $D' \leq D_{\max}(r)$ with $D_{\max}(r)$ defined in the statement of the lemma. Since $D' \geq 10^{19}$ and $D_{\max}(r) \leq 10^{10}$ for $r \leq 10$ we must have $r > 10$ and thus $D' \leq D_{\max}(r) = 2^r r! \leq r^r$ and $n\log n \leq l(4D')\log l(4D') \leq \log D' \leq r\log r$ which ensures that $n \leq r$.

By assumption $r \leq r(\alpha')$. Thus there exist at least n multiplicatively independent conjugates of α', say $\alpha'_1, \ldots, \alpha'_n$. Theorem 1.5 shows that $h(\alpha') \geq e^{-U}$ where

$$U = \frac{1}{n}\log D_{\mathrm{ab}} + \frac{1}{n}\log(c_2(n)) + \frac{\kappa_2(n)}{n}\log\log(16D_{\mathrm{ab}}) \tag{3.4}$$

and with $c_2(n)$ and $\kappa_2(n)$ defined in that theorem.

We have to prove (3.2). Since $n \geq 12$, an elementary computation shows that

$$\frac{1}{n}\log(c_2(n)) = \log(2n^2) + 64n\cdot n!\left(2(n+1)^2(n+1)!\right)^{2n} \leq n^{2n^2}$$

and

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

Thus (taking into account $n \ge x-1 \ge \frac{x}{2}$)

$$\begin{aligned} U &\le \left(\frac{1}{n} + \frac{2n^{2n^2}\log\log(16D_{\mathrm{ab}})}{\log(16D_{\mathrm{ab}})}\right)\log(16D_{\mathrm{ab}}) \\ &\le 4\max\left\{\frac{1}{x}, x^{2x^2} l(16D_{\mathrm{ab}})^{-1}\right\}\log(16D_{\mathrm{ab}}). \end{aligned} \tag{3.5}$$

We now quote the following inequality, which can be easily checked.

Fact. *For $t \ge 16$ we have*

$$\frac{1}{2}\left(1 + \frac{1}{18}l_2(t)\right)\log(l_2(t)/36) \le \log l(t).$$

Since $x \le \frac{1}{6}l_2(16D_{\mathrm{ab}})^{1/2}$, by the fact above we have

$$(1+2x^2)\log x \le \frac{1}{2}\left(1 + \frac{1}{18}l_2(16D_{\mathrm{ab}})\right)\log(l_2(16D_{\mathrm{ab}})/36) \le \log l(16D_{\mathrm{ab}}).$$

Thus $x^{1+2x^2} \le l(16D_{\mathrm{ab}})$ and, by (3.5),

$$\begin{aligned} U \le \frac{4}{x}\log(16D_{\mathrm{ab}}) &= 4\max\left\{6l_2(16D_{\mathrm{ab}})^{-1/2},\ l(16D')^{-1}\right\}\log(16D_{\mathrm{ab}}) \\ &\le 72\cdot 10^3 \max\left\{l_2(16D_{\mathrm{ab}})^{-1/2},\ l(16D')^{-1}\right\}\log(16D_{\mathrm{ab}}). \end{aligned}$$

Inequality (3.2) is proved.

□

It is interesting to compare Theorem 3.1 with [2, Corollary 3.2] which in the present situation shows that

$$h(\alpha') \ge c(\varepsilon)D^{-1/2-\varepsilon}$$

for any $\varepsilon > 0$, with $c(\varepsilon) > 0$. The result I) of Theorem 3.1 is asymptotically stronger, but only when D' is large.

Corollary 3.2. *Let α be a non zero algebraic number which is not a root of unity.*
I) Let us assume $\mathbb{Q}(\alpha^{e(\alpha)}) = \mathbb{Q}(\alpha)$. Then, for every $\alpha' \in \mathbb{Q}(\alpha)$ such that $r(\alpha') \ge r(\alpha)$ we have

$$h(\alpha') \ge e^{-U} \text{ with } U \le 8l(4D)^{-1/4}\log(4D)$$

where D is the degree of the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$.
II) Let us assume $\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)}) = \mathbb{Q}^{\mathrm{ab}}(\alpha)$. Then, for every $\alpha' \in \mathbb{Q}^{\mathrm{ab}}(\alpha)$ such that $r(\alpha') \ge r(\alpha)$ we have

$$h(\alpha') \ge e^{-U} \text{ with } U \le 3\cdot 72\cdot 10^3 l_2(16D_{\mathrm{ab}})^{-1/2}\log(16D_{\mathrm{ab}})$$

where D_{ab} is the degree of the normal closure of $\mathbb{Q}^{\mathrm{ab}}(\alpha)/\mathbb{Q}^{\mathrm{ab}}$.

Proof. Let D' and D'_{ab} be respectively the degrees of the normal closures of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$ and of $\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})/\mathbb{Q}^{\mathrm{ab}}$.

We prove I). We apply Theorem 3.1 I), taking into account $D' = D$. Since $l(4D) \geq 1$, by assertion I) of that theorem we have $h(\alpha) \geq e^{-U}$ with

$$U = 8 \max\left\{ l(4D)^{-1/4},\ l(4D)^{-1} \right\} \log(4D) = 8 l(4D)^{-1/4} \log(4D).$$

Similarly, by Theorem 3.1, II) we have $h(\alpha) \geq e^{-U}$ with

$$U = 72 \cdot 10^3 \max\left\{ l_2(16D_{\mathrm{ab}})^{-1/2},\ l(16D')^{-1} \right\} \log(16D_{\mathrm{ab}}).$$

We now prove II). By assumption $D'_{\mathrm{ab}} = D_{\mathrm{ab}}$. Since $D' \geq D'_{\mathrm{ab}}$ we have $D' \geq D_{\mathrm{ab}}$. A computation shows that $l_2(t)^{1/2} \leq 3l(t)$ for $t \geq 16$. Thus $l_2(16D_{\mathrm{ab}})^{1/2} \leq 3l(16D_{\mathrm{ab}}) \leq 3l(16D')$ (by Remark 2.3 i) and since $D_{\mathrm{ab}} \leq D'$) and

$$U \leq 3 \cdot 72 \cdot 10^3 l_2(16D_{\mathrm{ab}})^{-1/2} \log(16D_{\mathrm{ab}}).$$

□

The assumption $\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)}) = \mathbb{Q}^{\mathrm{ab}}(\alpha)$ of part II) of the previous corollary, is easily read on the minimal polynomial of α over $\mathbb{Q}$. This not seem to be the case for the analogous assumption $\mathbb{Q}(\alpha^{e(\alpha)}) = \mathbb{Q}(\alpha)$ of part I).

Lemma 3.3. *Let α be an algebraic number with minimal polynomial $P(X)$ over $\mathbb{Q}$. Let us assume that P is not a polynomial in X^δ for δ integer > 1. Then for any integer $e \geq 1$ we have $\mathbb{Q}^{\mathrm{ab}}(\alpha^e) = \mathbb{Q}^{\mathrm{ab}}(\alpha)$.*

Proof. Let $e \geq 1$ be an integer. Let for short $E = \mathbb{Q}^{\mathrm{ab}}(\alpha^e) \cap \mathbb{Q}(\alpha)$. We note $\delta = [\mathbb{Q}(\alpha) : E]$ and $\alpha' = \mathrm{Norm}_E^{\mathbb{Q}(\alpha)}(\alpha) \in E$. Thus $\alpha' = \zeta \alpha^\delta$ for some root of unity ζ. Hence $\zeta \in \mathbb{Q}^{\mathrm{ab}}$. Since $\zeta = \alpha'/\alpha^\delta \in \mathbb{Q}(\alpha)$ we have $\zeta \in \mathbb{Q}^{\mathrm{ab}} \cap \mathbb{Q}(\alpha) \subseteq E$ and thus also $\alpha^\delta \in E$. Let

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

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.

□

4. 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 1.3 from it.

Theorem 4.1. *Let $\gamma_0, \gamma_1, \dots \gamma_k \in \overline{\mathbb{Q}}^*$ and $m_0, \dots, m_k \in \mathbb{Z}$ with $0 = m_k < m_{k-1} < \cdots < m_1 < m_0$. We set $h^* = h^*(\boldsymbol{\gamma}) := k(h(\gamma_0 : \cdots : \gamma_k) + \log k)$. Let α be a root of the polynomial*

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

of degree $d := m_0$. We assume that α is not a root of unity and that there is no vanishing subsum of the form $\gamma_0 \alpha^{m_0} + \cdots + \gamma_l \alpha_l^{m_l}$ with $l < k$.
I) If $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^{e(\alpha)})$ and $d \geq 3h^*$, the degree D of the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ satisfies

$$\log(4D) > 6^{-1} l(d/h^*)^{1/3} \log(d/h^*). \tag{4.1}$$

II) If $\mathbb{Q}^{\mathrm{ab}}(\alpha) = \mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})$ *and* $d \geq 16h^*$*, the degree* D_{ab} *of the Galois closure of* $\mathbb{Q}^{\mathrm{ab}}(\alpha)/\mathbb{Q}^{\mathrm{ab}}$ *satisfies*

$$\log(16D_{\mathrm{ab}}) > 10^{-7} l_2(d/h^*)^{1/2} \log(d/h^*). \tag{4.2}$$

Proof. By the assumption on non-vanishing subsums, we can apply [6, Lemma 2.2] to get

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

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

$$h(\alpha) \leq \exp(-\log(d/h^*)). \tag{4.3}$$

Let us prove I). By Corollary 3.2 I) $h(\alpha) \geq e^{-U}$ with

$$U \leq 8l(4D)^{-1/4} \log(4D) = 8(\log 4D)^{3/4} (\log\log 4D)^{1/4}.$$

Comparing with (4.3) we get $8(\log 4D)^{3/4}(\log\log 4D)^{1/4} \geq \log(d/h^*)$, *i. e.*

$$\log(4D) \geq 8^{-3/4} (\log\log(4D))^{-1/3} (\log(d/h^*))^{4/3}. \tag{4.4}$$

If $\log(4D) \geq \log(d/h^*)^{4/3}$ then (4.1) is obviously satisfied (since $d/h^* \geq 3$ and $6^{-1}\log\log(3)^{-1/3} < 1$). Otherwise, we have $\log\log(4D) \leq \frac{4}{3}\log\log(d/h^*)$ and then (4.4) implies again (4.1):

$$\begin{aligned} \log(4D) &\geq 8^{-3/4}(4/3)^{-1/3} (\log\log(d/h^*))^{-1/3} (\log(d/h^*))^{4/3} \\ &> 6^{-1} l(d/h^*)^{1/3} \log(d/h^*). \end{aligned}$$

Let now prove II). By Corollary 3.2 II)

$$h(\alpha') \geq e^{-U} \text{ with } U \leq 3 \cdot 72 \cdot 10^3 l_2(16D_{\mathrm{ab}})^{-1/2} \log(16D_{\mathrm{ab}}).$$

Comparing with (4.3) we get

$$c \log(16D_{\mathrm{ab}}) \geq l_2(16D_{\mathrm{ab}})^{1/2} \log(d/h^*). \tag{4.5}$$

with $c = 3 \cdot 72 \cdot 10^3$. Since $l_2(16D_{\mathrm{ab}}) \geq 1$, this implies $\log(d/h^*) \leq c \log(16D_{\mathrm{ab}})$. Since $d/h^* \geq 16$, from Remark 2.3 i) we get

$$l_2(d/h^*) = l(\log(d/h^*)) \leq e^{-1} l_2(16) l(c \log(16D_{\mathrm{ab}})).$$

A direct computation shows that $l(c \cdot t) \leq 3l(t)$ for $t > e$. Thus

$$l_2(d/h^*) \leq 3e^{-1} l_2(16) l(\log(16D_{\mathrm{ab}})) \leq 8^2 l_2(16D_{\mathrm{ab}}).$$

Inserting this inequality in (4.5) we get

$$\log(16D) \geq (8 \cdot c)^{-1} l_2(d/h^*)^{1/2} \log(d/h^*) > 10^{-7} l_2(d/h^*)^{1/2} \log(d/h^*).$$

□

Proof of Theorem 1.3. We fix a positive integer k and non zero $\gamma_1, \dots, \gamma_k \in \mathbb{Z}$. Let $m_0, \dots, m_k \in \mathbb{Z}$ coprime with $0 = m_k < \cdots < m_0 =: d$ and with $d \to +\infty$. 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. 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 $l < k$. Moreover, we can assume $P_{\mathbf{m}}$ not cyclotomic (since the number of non zero coefficients of a cyclotomic polynomial with coprime exponents growth to infinity with the degree Thus 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 3.3, $\mathbb{Q}^{\mathrm{ab}}(\alpha) = \mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})$. All the assumptions of Theorem 4.1 II) are now satisfied. From 4.2 and Remark 2.3 ii) we get:

$$\log(16 D_{\mathrm{ab}}) > 10^{-7} l_2 (d/h^*)^{1/2} \log(d/h^*) \geq 10^{-7} \log\log(d/h^*)^{1/4} \log(d/h^*).$$

□

Remark 4.2. *The assumption on the coprimality of the exponents is not enough to ensure $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^{e(\alpha)})$. Thus, even for a lower bound of the size of the Galois group over $\mathbb{Q}$, we need assertion II) of Theorem 5.1 and thus the lower bound of Theorem 1.5.*

5. Lehmer's problem and Galois groups

Theorem 1.2 announced in the introduction is a special case of the following result.

Theorem 5.1. *Let α be a non zero algebraic number which is not a root of unity. I) Let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, $d' = [\mathbb{Q}(\alpha^{e(\alpha)}) : \mathbb{Q}]$ and let D be the degree of the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$. Let us assume*

$$\log(4D) \leq c^{-1} \min\left\{ l(\rho d)^{1/3}, l(\rho d')^{4/3} \right\} \log(\rho d). \tag{5.1}$$

for some $\rho \geq 4$, where $c = 500$. Then, if α is not a root of unity,

$$h(\alpha) \geq \frac{1}{\rho d}.$$

II) Let $d_{\mathrm{ab}} = [\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}]$, $d'_{\mathrm{ab}} = [\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)}) \cap \mathbb{Q}(\alpha) : \mathbb{Q}^{\mathrm{ab}} \cap \mathbb{Q}(\alpha)]$ and let D_{ab} be the degree of the normal closure of $\mathbb{Q}^{\mathrm{ab}}(\alpha)/\mathbb{Q}^{\mathrm{ab}}$. Let us assume

$$\log(16 D_{\mathrm{ab}}) \leq c^{-1} \min\left\{ l_2(\rho d_{\mathrm{ab}})^{1/2}, l(\rho d'_{\mathrm{ab}}) l_2(\rho d'_{\mathrm{ab}})^{1/2} \right\} \log(\rho d_{\mathrm{ab}}). \tag{5.2}$$

for some $\rho \geq 16$, where $c = 2 \cdot 10^{11}$. Then, if α is not a root of unity,

$$h(\alpha) \geq \frac{1}{\rho d_{\mathrm{ab}}}.$$

Proof. The strategy of the proof of I) is the following. We forget for the moment the parameter ρ, the constants and the factors $\log\log$. Let D' be the degree of the normal closure of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$. If $\log D' \geq (\log D)/(\log d)$, Theorem 3.1 with $\alpha' = \alpha$ gives a lower bound of the shape $h(\alpha) \geq e^{-U}$ with $U \leq (\log D)^{3/4}$, which implies the desired result, by the upper bound $\log D \leq (\log d)^{4/3}$ of (5.1). Otherwise, we

apply Theorem 3.1 (more precisely, its corollary 3.2) with $\alpha^{e(\alpha)}$ at the place of α, choosing

$$\alpha' = \mathrm{Norm}^{\mathbb{Q}(\alpha)}_{\mathbb{Q}(\alpha^{e(\alpha)})}(\alpha) = (\text{root of unity}) \cdot \alpha^{d/d'}.$$

This gives the lower bound $h(\alpha') \geq e^{-U}$ with $U \leq (\log D')^{3/4}$. Since we are now assuming $\log D' \leq (\log D)/(\log d)$ and $\log D \leq (\log d')^{4/3} \log d$ by (5.1), we obtain a "Lehmer's type" lower bound $h(\alpha') \geq 1/d'$ for the height of α' and thus a "Lehmer's type" lower bound $h(\alpha) \geq 1/d$ for the height of α.

The proof of II) follows a similar pattern, with some more technical complications.

We prove I). Let D' be the degree of the normal closure of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$. Let us assume first

$$8l(4D')^{-1} \log(4D) \leq \log(\rho d). \tag{5.3}$$

By Theorem 3.1 (with $\alpha' = \alpha$)

$$h(\alpha) \geq e^{-U}, \text{ with } U = 8 \max\left\{l(4D)^{-1/4},\ l(4D')^{-1}\right\} \log(4D). \tag{5.4}$$

By (5.1), $\log(4D) \leq 500^{-1} l(\rho d)^{1/3} \log(\rho d) = 500^{-1} \log(\rho d)^{4/3} \log\log(\rho d)^{-1/3}$, which in turn implies (taking into account $500^{-1}(\log\log 4)^{-1/3} \leq 1$)

$$\log\log(4D) \leq \frac{4}{3} \log\log(\rho d).$$

Thus

$$\begin{aligned} 8l(4D)^{-1/4} \log(4D) &= 8(\log(4D))^{3/4} (\log\log(4D))^{1/4} \\ &\leq 8 \cdot 500^{-3/4} \log(\rho d) \log\log(\rho d)^{-1/4} \cdot (4/3)^{1/4} \log\log(\rho d)^{1/4} < \log(\rho d). \end{aligned} \tag{5.5}$$

By (5.4), (5.5) and (5.3) we get $h(\alpha) \geq \frac{1}{\rho d}$.

Let now assume

$$8l(4D')^{-1} \log(4D) > \log(\rho d). \tag{5.6}$$

We have $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^{e(\alpha)})] = d/d'$. Thus,

$$\alpha' := \mathrm{Norm}^{\mathbb{Q}(\alpha)}_{\mathbb{Q}(\alpha^{e(\alpha)})}(\alpha) = (\text{root of unity}) \cdot \alpha^{d/d'}.$$

In particular, $\alpha' \in \mathbb{Q}(\alpha^{e(\alpha)})$ and $r(\alpha') = r(\alpha) = r(\alpha^{e(\alpha)})$. Moreover, the multiplicative group generated by the conjugates of $\alpha^{e(\alpha)}$ has no torsion, *i. e.* $e(\alpha^{e(\alpha)}) = 1$. Thus applying By Corollary 3.2 (with $\alpha^{e(\alpha)}$ at the place of α) we get

$$h(\alpha') \geq e^{-U}, \text{ with } U = 8l(4D')^{-1/4} \log(4D') = 8l(4D')^{3/4} \log\log(4D').$$

By (5.1), $\log(4D) \leq 500^{-1} l(\rho d')^{4/3} \log(\rho d)$. Thus (5.6) gives

$$l(4D') < 8 \log(4D) \log(\rho d)^{-1} \leq 60^{-1} l(\rho d')^{4/3}$$

which in turn implies $\log(4D')^{1/2} \leq \log(\rho d')^{4/3}$ (by Remark 2.3 ii) and since $60^{-1}(\log\log 4)^{-4/3} \leq 1$) and

$$\log\log(4D') \leq \frac{8}{3} \log\log(\rho d').$$

We get:

$$U \leq 8 \cdot 60^{-3/4} l(\rho d') \cdot \frac{8}{3} \log\log(\rho d') < \log(\rho d').$$

This gives

$$h(\alpha) = \frac{d'}{d} h(\alpha') \geq \frac{d'}{d} e^{-U} \geq \frac{1}{\rho d}.$$

We now prove II). Let D'_{ab} be the degree of the normal closure of $\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})/\mathbb{Q}^{\mathrm{ab}}$ and let for short $c_0 = 72 \cdot 10^3$. Let us assume first

$$l(16D'_{\mathrm{ab}})^{-1} \log(16D_{\mathrm{ab}}) \leq c_0^{-1} \log(\rho d_{\mathrm{ab}}). \tag{5.7}$$

By II) of Theorem 3.1 (with $\alpha' = \alpha$, and since the degree D' of the normal closure of $\mathbb{Q}(\alpha^{e(\alpha)})/\mathbb{Q}$ is bounded by D'_{ab}), $h(\alpha) \geq e^{-U}$ with

$$U = c_0 \max\left\{ l_2(16D_{\mathrm{ab}})^{-1/2},\ l(16D'_{\mathrm{ab}})^{-1} \right\} \log(16D_{\mathrm{ab}}). \tag{5.8}$$

In order to show that $h(\alpha) \geq \frac{1}{\rho d_{\mathrm{ab}}}$ we quote the following tedious computation:

Fact.

$$U \leq \log(\rho d_{\mathrm{ab}})$$

Proof. By (5.8) and (5.7), it enough to prove that

$$\log(16D_{\mathrm{ab}}) \leq c_0^{-1} l_2(16D_{\mathrm{ab}})^{1/2} \log(\rho d_{\mathrm{ab}}). \tag{5.9}$$

This is clear if $\log(16D_{\mathrm{ab}}) \leq c_0^{-1} \log(\rho d_{\mathrm{ab}})$, since $l_2(16D_{\mathrm{ab}}) \geq 1$. If otherwise $\log(\rho d_{\mathrm{ab}}) \leq c_0 \log(16D_{\mathrm{ab}})$, then

$$\begin{aligned} l_2(\rho d_{\mathrm{ab}})^{1/2} \log(\rho d_{\mathrm{ab}}) &= l(\log(\rho d_{\mathrm{ab}}))^{1/2} \log(\rho d_{\mathrm{ab}}) \\ &\leq \left(e^{-1} l_2(16)\right)^{1/2} l(c_0 \log(16D_{\mathrm{ab}}))^{1/2} \log(\rho d_{\mathrm{ab}}) \end{aligned}$$

by Remark 2.3. Moreover a direct computation shows that $l(\log(c_0 t)) \leq 2l(t)$ for $t > e$. Thus

$$l_2(\rho d_{\mathrm{ab}})^{1/2} \log(\rho d_{\mathrm{ab}}) \leq \left(2e^{-1} l_2(16)\right)^{1/2} l_2(16D_{\mathrm{ab}})^{1/2} \log(\rho d_{\mathrm{ab}}).$$

Inequality (5.9) now follows from (5.2):

$$\log(16D_{\mathrm{ab}}) \leq c^{-1} l_2(\rho d_{\mathrm{ab}})^{1/2} \log(\rho d_{\mathrm{ab}}) \leq c_0^{-1} l_2(16D_{\mathrm{ab}})^{1/2} \log(\rho d_{\mathrm{ab}})$$

since $\left(2e^{-1} l_2(16)\right)^{1/2} c_0 \leq 7 \cdot 72 \cdot 10^3 \leq 2 \cdot 10^{11} = c$.

□

Let now assume

$$l(16D'_{\mathrm{ab}})^{-1} \log(16D_{\mathrm{ab}}) > c_0^{-1} \log(\rho d_{\mathrm{ab}}). \tag{5.10}$$

We have $[\mathbb{Q}(\alpha) : \mathbb{Q}^{\mathrm{ab}} \cap \mathbb{Q}(\alpha)] = [\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}] = d_{\mathrm{ab}}$. Thus, by definition of d'_{ab},

$$\alpha' := \mathrm{Norm}^{\mathbb{Q}(\alpha)}_{\mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)}) \cap \mathbb{Q}(\alpha)}(\alpha) = (\text{root of unity}) \cdot \alpha^{d_{\mathrm{ab}}/d'_{\mathrm{ab}}}.$$

In particular, $\alpha' \in \mathbb{Q}^{\mathrm{ab}}(\alpha^{e(\alpha)})$ and $r(\alpha') = r(\alpha) = r(\alpha^{e(\alpha)})$. As in the proof of part I), $e(\alpha^{e(\alpha)}) = 1$ and we can apply Corollary 3.2 (with $\alpha^{e(\alpha)}$ at the place of α). We get $h(\alpha') \geq e^{-U}$ with

$$U \leq 3c_0 l_2(16D'_{\mathrm{ab}})^{-1/2} \log(16D'_{\mathrm{ab}}). \tag{5.11}$$

We need an other tedious computation:

Fact.

$$U \leq \log(\rho d'_{\mathrm{ab}}).$$

Proof. Let for short $u(t) = (\log\log(t)\log\log\log(t))^{1/2} = l(t)^{-1}l_2(t)^{-1/2}\log(t)$. Thus (5.11) becomes

$$U \leq 3c_0 u(16D'_{\mathrm{ab}})l(16D'_{\mathrm{ab}}). \tag{5.12}$$

By (5.2),

$$\begin{aligned}\log(16D_{\mathrm{ab}}) &\leq c^{-1}l(\rho d'_{\mathrm{ab}})l_2(\rho d'_{\mathrm{ab}})^{1/2}\log(\rho d_{\mathrm{ab}}) \\ &= c^{-1}u(\rho d'_{\mathrm{ab}})^{-1}\log(\rho d'_{\mathrm{ab}})\log(\rho d_{\mathrm{ab}})\end{aligned}$$

Thus, by (5.10) and since $c = 2\cdot 10^{11} > 27\cdot c_0^2$,

$$\begin{aligned}l(16D'_{\mathrm{ab}}) &< c_0\log(16D_{\mathrm{ab}})\log(\rho d_{\mathrm{ab}})^{-1} \\ &\leq (27\cdot c_0)^{-1}u(\rho d'_{\mathrm{ab}})^{-1}\log(\rho d'_{\mathrm{ab}})\end{aligned} \tag{5.13}$$

which in turn implies $\log\log(16D'_{\mathrm{ab}}) \leq 2\log\log(\rho d'_{\mathrm{ab}})$ (taking into account $(27\cdot c_0)^{-1}u(16) \leq 1$ and Remark 2.3 ii)) and

$$\log\log\log(16D'_{\mathrm{ab}}) \leq \left(1 + \frac{\log 2}{\log\log\log 16}\right)\log\log\log(\rho d'_{\mathrm{ab}}) \leq 37\log\log\log(\rho d'_{\mathrm{ab}}).$$

Thus $u(16D'_{\mathrm{ab}}) \leq \sqrt{2\cdot 37}\,u(\rho d'_{\mathrm{ab}}) \leq 9u(\rho d'_{\mathrm{ab}})$. From this last inequality and from (5.12) and (5.13) we get

$$U \leq 3c_0\cdot 9u(\rho d'_{\mathrm{ab}})\cdot(27\cdot c_0)^{-1}u(\rho d'_{\mathrm{ab}})^{-1}\log(\rho d'_{\mathrm{ab}}) = \log(\rho d'_{\mathrm{ab}}).$$

□

By the fact above,

$$h(\alpha) = \frac{d'_{\mathrm{ab}}}{d_{\mathrm{ab}}}h(\alpha') \geq \frac{d'_{\mathrm{ab}}}{d_{\mathrm{ab}}}e^{-U} \geq \frac{1}{\rho d_{\mathrm{ab}}}.$$

□

Proof of Theorem 1.2. We apply Theorem 5.1, I). Since $d_0 \leq d' \leq d$ and $\rho \geq 16$, we have by Remark 2.3,

$$\min\{l(\rho d)^{1/3}, l(\rho d')^{4/3}\} \geq l(\rho d_0)^{1/3} \geq \log(\rho d_0)^{1/6}.$$

□

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 D. Masser, "Lower bounds for the height in Galois extensions", *Bull. London Math. Soc.* **48** (2016), 1008–1012.
3. F. Amoroso and E. Viada, "Small points on rational subvarieties of tori", *Comment. Math. Helv.* **87** (2012), 355–383
4. N. Berry, A. Dubickas, N. Elkies, B. Poonen and C. Smyth, "The conjugate dimension of algebraic numbers" *Q. J. Math.* **55** (2004), no. 3, 237–252.
5. M. Bardestani, private communication, Workshop on Heights and Applications to Unlikely Intersections, February 13 - 17, 2017, The Fields Institute, Toronto.
6. P. Corvaja and U. Zannier, *On the rank of certain matrices*, Math. Nachr. **284** (2011), 1652–1657.

7. E. Delsinne, "Le problème de Lehmer relatif en dimension supérieure", *Ann. Sci. École Norm. Sup.* **42**, fascicule 6 (2009), 981–1028.
8. E. Dobrowolski, "On a question of Lehmer and the number of irreducible factors of a polynomial", *Acta Arith.*, **34** (1979), 391–401.
9. W. Feit, "The orders of finite linear groups". Preprint 1995.
10. S. Friedland, "The maximal orders of finite subgroups in $\mathrm{GL}_n(\mathbb{Q})$", *Proc. Amer. Math. Soc.* **125** (1997), 3519–3526.
11. U. Rausch, "On a theorem of Dobrowolski about the product of conjugate numbers." *Colloq. Math.* **50** (1985), no. 1, 137–142.
12. P. Voutier "An effective lower bound for the height of algebraic numbers". *Acta Arith.* **74** (1996), no. 1, 81–95.