Mahler measure on Galois extensions

Francesco Amoroso

MAHLER MEASURE ON GALOIS EXTENSIONS.

FRANCESCO AMOROSO

Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen, Campus II, BP 5186
14032 Caen Cedex, France

Abstract. We study the Mahler measure of generators of a Galois extension with Galois group the full symmetric group. We prove that two classical constructions of generators gives always algebraic numbers of big height. These results answer a question of C. Smyth and provide some evidence to a conjecture which asserts that the height of such a generator growth to infinity with the degree of the extension.

1. Introduction

Let α be a non-zero algebraic number of degree d. We let as usual $M(\alpha)$ the Mahler measure of α. Thus

$$M(\alpha) = |\mathrm{lc}(f)| \prod_{j=1}^{d} \max(|\alpha_j|, 1)$$

where $\mathrm{lc}(f)$ is the leading coefficient of a minimal equation of α over $\mathbb{Z}$ and where $\alpha_1, \ldots, \alpha_d$ are the conjugates of α.

Assume that α is not a root of unity (otherwise $M(\alpha) = 1$). By an old result of Kronecker $M(\alpha) > 1$ and Lehmer [5] asked if we could replace 1 by a real number > 1 which does not depend on α. This problem is still open, the best known result is a theorem of Dobrowolski (see [4]) which proves the lower bound

$$M(\alpha) \geq 1 + c(\varepsilon) d^{-\varepsilon}$$

for all $\varepsilon > 0$, with $c(\varepsilon) > 0$ depending only on ε.

Recently, a construction of Smyth gives a renewed interest in lower bounds for the Mahler measure of a *generator* of a Galois extension (a problem first considered in [1]). In this special case we can considerably improve the above lower bound. Let α be a non-zero algebraic number of degree d, not a root unity, such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Then (see [2])

$$M(\alpha)^{1/d} \geq 1 + c(\varepsilon) d^{-\varepsilon}$$

for all $\varepsilon > 0$, with $c(\varepsilon) > 0$ depending only on ε.

The result of [2] was partially motivated by a problem posed by Smyth during a recent BIRS workshop (see [3, problem 21, p. 17]). Let $n \geq 2$ and $\beta = \beta_1, \ldots, \beta_n$ be the roots of $z^n - z - 1$, known to be irreducible for all n, and to have Galois group the full symmetric group $\mathfrak{S}_n$. Put

$$\alpha = \beta_1^1 \beta_2^2 \ldots \beta_{n-1}^{n-1}.$$

Date: 20 august 2017.

Then (by an easy consequence of [6] Lemma 1) the Galois closure of $\mathbb{Q}(\beta)$ is $\mathbb{Q}(\alpha)$ of degree $d = n!$ over $\mathbb{Q}$. Smyth computed with Maple the first values of $M(\alpha)^{1/d}$

n	$d = n!$	$M(\alpha)^{1/d}$
2	2	1.2720196495
3	6	1.1509639252
4	24	1.2428334720
5	120	1.2292495215
6	720	1.2846087150
7	5040	1.2833028970
8	40320	1.3243452986
9	362880	1.3307248410

and asked the following questions:

(1) Does anyone know of any smaller values of $M(\alpha)^{1/d} > 1$ for α of degree d with $\mathbb{Q}(\alpha)$ Galois?
(2) Does the above sequence of values $M(\alpha)^{1/d}$ tend to a limit as $n \to \infty$ and, if so, what is it?

The quoted result of [2] is related to the first question. One of the aim of this paper is to give an answer to the second question. More generally, in section 3 we show:

Theorem 1.1. *Let β be an algebraic unit of degree n, with algebraic conjugates $\beta_1, \dots, \beta_n$. Assume that $\mathbb{Q}(\beta_1, \dots, \beta_n)/\mathbb{Q}$ has Galois group $\mathfrak{S}_n$. Let $a_1, \dots, a_n \in \mathbb{Z}$ and put*

$$\alpha = \beta_1^{a_1} \beta_2^{a_2} \cdots \beta_n^{a_n}.$$

Then:

1) *α is a generator of $\mathbb{Q}(\beta_1, \dots, \beta_n)/\mathbb{Q}$ if and only if $a_1, \dots, a_n$ are pairwise distinct.*
2) *Put $y_j = a_j - \frac{1}{n}\sum_i a_i$. Then*

$$M(\beta)^{c_n |\mathbf{y}|_1} \le M(\alpha)^{1/n!} \le M(\beta)^{|\mathbf{y}|_1}$$

with $|\mathbf{y}|_1 = \frac{1}{n}\sum_{j=1}^n |y_j|$ and where $c_n \sim \sqrt{\frac{2}{\pi n}}$.
3) *If α is a generator of $\mathbb{Q}(\beta_1, \dots, \beta_n)/\mathbb{Q}$,*

$$M(\alpha)^{1/n!} \ge M(\beta)^{(1+o(1))\sqrt{\frac{n}{8\pi}}}.$$

The Mahler measure of a root of $x^n - x - 1$ is $\ge \theta = 1.32...$, the smallest Pisot's number (the root > 1 of $x^3 - x - 1$). Thus Theorem 1.1 implies that Smyth's sequence tends to ∞.

A more classical way to construct a generator for the Galois closure of $\mathbb{Q}(\beta)$ is given by the proof of the Primitive Element Theorem, thus taking a general linear combination of the conjugates of β. In section 4 we give a proof, based on a simple discriminant argument, of the following partial analogous of Theorem 1.1.

Theorem 1.2. *Let β be an algebraic integer of degree n, with algebraic conjugates $\beta_1, \dots, \beta_n$. Assume that $\mathbb{Q}(\beta_1, \dots, \beta_n)/\mathbb{Q}$ has Galois group $\mathfrak{S}_n$. Let $a_1, \dots, a_n \in \mathbb{Z}$*

and put

$$\alpha = a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n.$$

Then:

1) *α is a generator of $\mathbb{Q}(\beta_1, \ldots, \beta_n)/\mathbb{Q}$ if and only if $a_1, \ldots, a_n$ are pairwise distinct.*
2) *Let $V(\mathbf{a})$ be the Vandermonde $\prod_{1\le i<j\le n}(a_j - a_i)$. Then, if $n \ge 5$,*

$$2^{-\frac{1}{24}}\left(|V(\mathbf{a})| \cdot |\mathrm{disc}(\beta)|^{1/2}\right)^{\frac{1}{12n(n-1)}} \le M(\alpha)^{1/n!} \le |\mathbf{a}|_1 \cdot M(\beta).$$

3) *If α is a generator of $\mathbb{Q}(\beta_1, \ldots, \beta_n)/\mathbb{Q}$,*

$$M(\alpha)^{1/n!} \ge (n/4)^{1/48}.$$

Theorems 1.1 and 1.2 may suggest some speculations on the behavior of $M(\alpha)$ for α a generator of a Galois extension.

Conjecture 1.3. *Let $\alpha \in \overline{\mathbb{Q}}$ be a generator of of a Galois extension of degree $d = n!$ with Galois group the full symmetric group $\mathfrak{S}_n$. Then,*

$$M(\alpha)^{1/d} \ge C(d)$$

with $C(d) \to +\infty$ for $d \to +\infty$.

Equivalently, in terms of the Weil height $h(\alpha) = \frac{1}{d}\log M(\alpha)$,

$$h(\alpha) \ge c(d)$$

with $c(d)$ growing to infinity with d. This would be the first result of the kind "$h \to +\infty$".

Remark that the assumption on the Galois group is necessary, as a couple of exemples of [2] show: take ζ_e a e-root of unity and put $\alpha = 1 + \zeta_e$ or $\alpha = 2^{1/e} + \zeta_e$, both of uniformly bounded height.

Aknowledgements. We are indebted to Eric Ricard for a convexity argument which is the key of the proof of Lemma 2.2. We warmly thank Tanguy Rivoal for equality (2.3).

2. Auxiliary results

Let $H_n := \{\mathbf{x} \in \mathbb{R}^n \mid x_1 + \cdots + x_n = 0\}$ and, for $\mathbf{x} \in H_n$,

$$|\mathbf{x}|_1 = \frac{1}{n}\sum_{j=1}^{n} |x_j| .$$

We remark that $\mathfrak{S}_n$ acts on H_n (by $\sigma(\mathbf{x}) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$).

For $\mathbf{x}$, $\mathbf{y} \in H_n$ we set

$$s_n(\mathbf{x}, \mathbf{y}) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} \left|\frac{1}{n}\sum_{j=1}^{n} x_{\sigma(j)}y_j\right| .$$

Thus s_n is symmetric,

$$s_n(\mathbf{x},\mathbf{y}) = s_n(\mathbf{y},\mathbf{x}).$$

Moreover, for each $\mathbf{y} \in H_n$, the function $\mathbf{x} \mapsto s_n(\mathbf{x},\mathbf{y})$ is a seminorm[1], stable by the action on $\mathfrak{S}_n$.

For $h = 1, \dots, n-1$ we define a vector $\mathbf{z}^{(n,h)} \in H_n$ by

$$z_j^{(n,h)} = \begin{cases} \frac{n}{2h} & \text{if } j = 1, \dots, h \\ -\frac{n}{2(n-h)} & \text{if } j = h+1, \dots, n \end{cases}$$

(thus $|\mathbf{z}^{(n,h)}|_1 = 1$). Let also

$$c_n = \min_{0<h,k<n} s_n(\mathbf{z}^{(n,h)}, \mathbf{z}^{(n,k)}).$$

The aim of this section is to prove the following proposition.

Proposition 2.1. *For $\mathbf{x}$, $\mathbf{y} \in H_n \backslash \{0\}$ we have*

$$c_n \le \frac{s_n(\mathbf{x},\mathbf{y})}{|\mathbf{x}|_1 \cdot |\mathbf{y}|_1} \le 1\ . \tag{2.1}$$

Moreover

$$c_n \sim \sqrt{\frac{2}{\pi n}}\ . \tag{2.2}$$

The above lower bound is clearly sharp, and the upper bound is almost sharp, since

$$s_n(\mathbf{z}^{(n,1)}, \mathbf{z}^{(n,k)}) = \frac{n}{2(n-1)}$$

(see Lemma 2.3 below).

Proposition 2.1 easily implies the lower bound for $M(\alpha)$ in assertion 2) of Theorem 1.1, as we shall see in the next session. In the rest of this section we present the proof of the proposition, which follows from the three lemmas below.

Lemma 2.2. *Let $\mathbf{x}$, $\mathbf{y} \in H_n \backslash \{0\}$. Let $h = h(\mathbf{x})$ be the cardinality of the set of $j \in \{1, \dots, n\}$ such that $x_j \ge 0$ and similarly for $k = k(\mathbf{y})$. Then*

$$\frac{s_n(\mathbf{x},\mathbf{y})}{|\mathbf{x}|_1 \cdot |\mathbf{y}|_1} \ge \frac{s_n(\mathbf{z}^{(n,h)},\mathbf{y})}{|\mathbf{y}|_1} \ge s_n(\mathbf{z}^{(n,h)}, \mathbf{z}^{(n,k)}).$$

Proof. Let us prove the first inequality. Since $\mathbf{x} \mapsto s_n(\mathbf{x},\mathbf{y})$ is homogeneous, we can assume $|\mathbf{x}|_1 = 1$. Let $\mathcal{A}$ be the set of $j \in \{1, \dots, n\}$ such that $x_j \ge 0$. Since $\mathbf{x} \mapsto s_n(\mathbf{x},\mathbf{y})$ is invariant by the action of $\mathfrak{S}_n$, we can assume $\mathcal{A} = \{1, \dots, h\}$. We now use a convexity argument suggested by E. Ricard. Let G be the subgroup of $\sigma \in \mathfrak{S}_n$ such that $\sigma(\mathcal{A}) = \mathcal{A}$. Then

$$|G|^{-1} \sum_{\sigma \in G} \sigma(\mathbf{x}) = \mathbf{z}^{(n,h)}$$

and, by the convexity of $\mathbf{x} \mapsto s_n(\mathbf{x},\mathbf{y})$,

$$s_n(\mathbf{z}^{(n,h)},\mathbf{y}) \le s_n(\mathbf{x},\mathbf{y}).$$

[1] and indeed a norm if $\mathbf{y} \neq 0$, for instance as a consequence of Proposition 2.1 below.

The second inequality follows from the first one and from the symmetry of s_n:

$$\frac{s_n(\mathbf{z}^{(n,h)},\mathbf{y})}{|\mathbf{y}|_1}=\frac{s_n(\mathbf{y},\mathbf{z}^{(n,h)})}{|\mathbf{y}|_1}\geq s_n(\mathbf{z}^{(n,k)},\mathbf{z}^{(n,h)})=s_n(\mathbf{z}^{(n,h)},\mathbf{z}^{(n,k)}).$$

□

Lemma 2.3. *Let $\mathbf{y}\in H_n$ and $h,\,k\in\{1,\dots,n\}$. Then*

$$s_n(\mathbf{z}^{(n,h)},\mathbf{y})=\frac{n}{2h(n-h)}\binom{n}{h}^{-1}\sum_{\substack{S\subseteq\{1,\dots,n\}\\ \mathrm{Card}(S)=h}}\Big|\sum_{j\in S}y_j\Big|$$

and

$$s_n(\mathbf{z}^{(n,h)},\mathbf{z}^{(n,k)})=\frac{n^2(h-[hk/n])(k-[hk/n])}{2hk(n-h)(n-k)}\binom{n}{h}^{-1}\binom{k}{[hk/n]}\binom{n-k}{h-[hk/n]}.$$

Proof. We have

$$\begin{aligned}
s_n(\mathbf{z}^{(n,h)},\mathbf{y})&=\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\left|\frac{1}{n}\sum_{j=1}^{n}z_j^{(n,h)}y_{\sigma(j)}\right|\\
&=\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\left|\frac{1}{2h}\sum_{j=1}^{h}y_{\sigma(j)}-\frac{1}{2(n-h)}\sum_{j=h+1}^{n}y_{\sigma(j)}\right|\\
&=\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\left|\left(\frac{1}{2h}+\frac{1}{2(n-h)}\right)\sum_{j=1}^{h}y_{\sigma(j)}\right|\\
&=\frac{n}{2h(n-h)}\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\left|\sum_{j=1}^{h}y_{\sigma(j)}\right|\\
&=\frac{n}{2h(n-h)}\binom{n}{h}^{-1}\sum_{\substack{S\subseteq\{1,\dots,n\}\\ \mathrm{Card}(S)=h}}\Big|\sum_{j\in S}y_j\Big|.
\end{aligned}$$

We now prove the second equality. From the first,

$$s_n(\mathbf{z}^{(n,h)},\mathbf{z}^{(n,k)})=\frac{n}{2h(n-h)}\binom{n}{h}^{-1}\sum_{\substack{S\subseteq\{1,\dots,n\}\\ \mathrm{Card}(S)=h}}\Big|\sum_{j\in S}z_j^{(n,k)}\Big|.$$

For $S\subseteq\{1,\dots,n\}$ of cardinality h we have

$$\begin{aligned}
\sum_{j\in S}z_j^{(n,k)}&=\frac{n}{2k}|S\cap\{1,\dots,k\}|-\frac{n}{2(n-k)}|S\cap\{k+1,\dots,n\}|\\
&=\left(\frac{n}{2k}+\frac{n}{2(n-k)}\right)|S\cap\{1,\dots,k\}|-\frac{n}{2(n-k)}|S|\\
&=\frac{n^2}{2k(n-k)}\Big(|S\cap\{1,\dots,k\}|-\frac{hk}{n}\Big).
\end{aligned}$$

This gives

$$s_n(\mathbf{z}^{(n,h)},\mathbf{z}^{(n,k)})=\frac{n^3}{4h(n-h)k(n-k)}\binom{n}{h}^{-1}\Sigma_{n,h,k}$$

with

$$\begin{aligned}\Sigma_{n,h,k} &= \sum_{\substack{S\subseteq\{1,\dots,n\}\\ \mathrm{Card}(S)=h}} \Big||S\cap\{1,\dots,k\}| - \frac{hk}{n}\Big| \\ &= \sum_{j=\max(h+k-n,0)}^{\min(h,k)} \Big(\sum_{\substack{S_1\subseteq\{1,\dots,k\}\\ \mathrm{Card}(S_1)=j}} 1\Big)\Big(\sum_{\substack{S_2\subseteq\{k+1,\dots,n\}\\ \mathrm{Card}(S_2)=h-j}} 1\Big)\Big|j-\frac{hk}{n}\Big| \\ &= \sum_{j=\max(h+k-n,0)}^{\min(h,k)} \binom{k}{j}\binom{n-k}{h-j}\Big|j-\frac{hk}{n}\Big|.\end{aligned}$$

We now quote an equality suggested by T. Rivoal. Let $q\in\mathbb{Z}$ with

$$\max(h+k-n,0)\le q\le \min(h,k).$$

Then

$$\sum_{j=\max(h+k-n,0)}^{q} \binom{k}{j}\binom{n-k}{h-j}\Big(\frac{hk}{n}-j\Big) = \frac{1}{n}(h-q)(k-q)\binom{k}{q}\binom{n-k}{h-q}. \tag{2.3}$$

This formula can be easily verified by induction on the parameter q. It shows that

$$\sum_{j=\max(h+k-n,0)}^{\min(h,k)} \binom{k}{j}\binom{n-k}{h-j}\Big(\frac{hk}{n}-j\Big) = 0$$

and that

$$\begin{aligned}\Sigma_{n,h,k} &= 2\sum_{j=\max(h+k-n,0)}^{[hk/n]} \binom{k}{j}\binom{n-k}{h-j}\Big(\frac{hk}{n}-j\Big) \\ &= \frac{2}{n}(h-[hk/n])(k-[hk/n])\binom{k}{[hk/n]}\binom{n-k}{h-[hk/n]}.\end{aligned}$$

Thus

$$\begin{aligned}s_n(\mathbf{z}^{(n,h)},\mathbf{z}^{(n,k)}) &= \frac{n^3}{4h(n-h)k(n-k)}\binom{n}{h}^{-1} \\ &\qquad\times\frac{2}{n}(h-[hk/n])(k-[hk/n])\binom{k}{[hk/n]}\binom{n-k}{h-[hk/n]} \\ &= \frac{n^2(h-[hk/n])(k-[hk/n])}{2hk(n-h)(n-k)}\binom{n}{h}^{-1}\binom{k}{[hk/n]}\binom{n-k}{h-[hk/n]}.\end{aligned}$$

□

In the next lemma we give an asymptotic estimate for

$$s_n(\mathbf{z}^{(n,h)},\mathbf{z}^{(n,k)}) = \frac{n^2(h-[hk/n])(k-[hk/n])}{2hk(n-h)(n-k)}\binom{n}{h}^{-1}\binom{k}{[hk/n]}\binom{n-k}{h-[hk/n]}.$$

Lemma 2.4. *Let $(n_m)_{n\in\mathbb{N}}$, $(h_m)_{m\in\mathbb{N}}$, $(k_m)_{m\in\mathbb{N}}$ with $0<h_m,k_m<n_m$. Assume*

$$\lim_{m\to+\infty} n_m = +\infty, \qquad \lim_{m\to+\infty}\frac{h_m}{n_m} = u, \qquad \lim_{m\to+\infty}\frac{k_m}{n_m} = v$$

for some $u, v \in [0,1]$. Then

$$\lim_{m\to+\infty} 2\sqrt{2\pi uv(1-u)(1-v)n_m}\cdot s_{n_m}(\mathbf{z}^{(n_m,h_m)},\mathbf{z}^{(n_m,k_m)}) = 1.$$

Proof. By a continuity argument, we can assume $u, v \in (0,1)$. Since

$$\lim_{m\to+\infty}\frac{[h_m k_m/n_m]}{n_m} = uv,$$

we have

$$\frac{n_m^2(h_m-[h_m k_m/n_m])(k_m-[h_m k_m/n_m])}{2h_m k_m(n_m-h_m)(n_m-k_m)} \sim \frac{(u-uv)(v-uv)}{2uv(1-u)(1-v)} = \frac{1}{2}.$$

For the other factors in $s_{n_m}(\mathbf{z}^{(n_m,h_m)},\mathbf{z}^{(n_m,k_m)})$ we use Stirling's formula, in the following version. Let $(n_m)_{m\in\mathbb{N}}$, $(A_m)_{m\in\mathbb{N}}$, $(B_m)_{m\in\mathbb{N}}$ with $0 \le B_m \le A_m$. Assume $n_m \to +\infty$, $A_m/n_m \to a$, $B_m/n_m \to b$ as $m \to +\infty$ with $0 < b < a$. Then

$$\binom{A_m}{B_m} \sim \frac{1}{\sqrt{2\pi n_m}} \times \sqrt{\frac{a}{b(a-b)}} \times \left(\frac{a^a}{b^b(a-b)^{a-b}}\right)^{n_m}.$$

Thus,

$$\binom{n_m}{h_m}^{-1} \sim \sqrt{2\pi n_m} \times \sqrt{u(1-u)} \times \left(u^u(1-u)^{1-u}\right)^{n_m}$$

and

$$\begin{aligned}\binom{k_m}{[h_m k_m/n_m]} &\sim \frac{1}{\sqrt{2\pi n_m}} \times \sqrt{\frac{v}{uv(v-uv)}} \times \left(\frac{v^v}{(uv)^{uv}(v-uv)^{v-uv}}\right)^{n_m} \\ &= \frac{1}{\sqrt{2\pi n_m}} \times \sqrt{\frac{1}{uv(1-u)}} \times \left(\frac{1}{u^{uv}(1-u)^{v-uv}}\right)^{n_m};\end{aligned}$$

$$\begin{aligned}\binom{n_m-k_m}{h_m-[h_m k_m/n_m]} &\sim \frac{1}{\sqrt{2\pi n_m}} \times \sqrt{\frac{1-v}{(u-uv)(1-v-u+uv)}} \\ &\qquad \times \left(\frac{(1-v)^{1-v}}{(u-uv)^{u-uv}(1-v-u+uv)^{1-v-u+uv}}\right)^{n_m} \\ &= \frac{1}{\sqrt{2\pi n_m}} \times \sqrt{\frac{1}{u(1-u)(1-v)}} \\ &\qquad \times \left(\frac{1}{u^{u-uv}(1-u)^{1-v-u+uv}}\right)^{n_m}.\end{aligned}$$

Hence

$$
\begin{aligned}
&s_{n_m}(\mathbf{z}^{(n_m,h_m)},\mathbf{z}^{(n_m,k_m)})\\
&\quad=\frac{n_m^2(h_m-[h_mk_m/n_m])(k_m-[h_mk_m/n_m])}{2h_mk_m(n_m-h_m)(n_m-k_m)}\\
&\qquad\qquad\times\binom{n_m}{h_m}^{-1}\binom{k_m}{[h_mk_m/n_m]}\binom{n_m-k_m}{h_m-[h_mk_m/n_m]}\\
&\quad\sim\frac{1}{2\sqrt{2\pi n_m}}\times\sqrt{u(1-u)\times\frac{1}{uv(1-u)}\times\frac{1}{u(1-u)(1-v)}}\\
&\qquad\qquad\times\left(u^u(1-u)^{1-u}\times\frac{1}{u^{uv}(1-u)^{v-uv}}\times\frac{1}{u^{u-uv}(1-u)^{1-v-u+uv}}\right)^{n_m}\\
&\quad=\frac{1}{2\sqrt{2\pi uv(1-u)(1-v)n_m}}.
\end{aligned}
$$

□

Proof of Proposition 2.1. The upper bound in (2.1) is easily proved:

$$
\begin{aligned}
\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\left|\frac{1}{n}\sum_{j=1}^{n}x_{\sigma(j)}y_j\right|&\le\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\frac{1}{n}\sum_{j=1}^{n}|x_{\sigma(j)}|\cdot|y_j|\\
&=\frac{1}{n}\sum_{j=1}^{n}\left(\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}|x_{\sigma(j)}|\right)|y_j|\\
&=\frac{1}{n}\sum_{j=1}^{n}|\mathbf{x}|_1\cdot y_j=|\mathbf{x}|_1\cdot|\mathbf{y}|_1.
\end{aligned}
$$

The lower bound follows from Lemma 2.2 and from the definition of c_n. The asymptotic estimate (2.2) for c_n is an easy consequence of Lemma 2.4, since

$$\max_{0\le u,v\le 1}uv(1-u)(1-v)=\frac{1}{16}.$$

□

3. Proof of Theorem 1.1

Let us prove the first assertion of the theorem. If $a_i=a_j$ for some $i\neq j$, then α is not a generator of $\mathbb{Q}(\beta_1,\dots,\beta_n)/\mathbb{Q}$, since $\tau\alpha=\alpha$ for $\tau=(i,j)$. Assume now $a_1,\dots,a_n$ pairwise distinct. Let σ be a permutation of $\mathfrak{S}_n$ such that $\sigma\alpha=\alpha$. Then

$$\beta_1^{a_1-a_{\sigma(1)}}\cdots\beta_n^{a_n-a_{\sigma(n)}}=1,$$

which implies, by [6, Lemma 1], that $j\mapsto a_j-a_{\sigma(j)}$ is constant, say $=\kappa$. For $l=o(\sigma)$ we have $a_1=a_{\sigma^l(1)}=\cdots=a_1+l\kappa$, thus $\kappa=0$ and $\forall j$, $a_{\sigma(j)}=a_j$. Since $a_1,\dots,a_n$ are pairwise distinct, σ is the identity.

To prove 2), let $x_j = \log|\beta_j| \in \mathbb{R}$ and remark that $\sum_j x_j = 0$ and $\sum_j |x_j| = 2\log M(\beta)$. Moreover

$$\frac{2}{n!}\log M(\alpha) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\left|\sum_{j=1}^{n} a_j x_{\sigma(j)}\right| = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\left|\sum_{j=1}^{n} x_{\sigma(j)} y_j\right|.$$

Inequality (2.1) of Proposition 2.1 then gives

$$c_n \frac{2\log M(\beta)}{n}|\mathbf{y}|_1 \le \frac{1}{n}\cdot\frac{2}{n!}\log M(\alpha) \le \frac{2\log M(\beta)}{n}|\mathbf{y}|_1$$

with $c_n \sim \sqrt{\frac{2}{\pi n}}$. Assertion 2) follows.

To prove the last assertion, we need the following elementary lemma:

Lemma. *Let $\mathbf{y} \in H_n$ with $y_{j+1} - y_j \ge 1$ for $j = 1, \dots, n-1$. Then*

$$|\mathbf{y}|_1 \ge \frac{n-2}{4}.$$

Proof. Let k be such that $y_k \le 0 < y_{k+1}$. Then, for $j = 1, \dots, k$

$$y_j \le y_k - (k-j) \le -(k-j)$$

while

$$y_j \ge y_{k+1} + (j-k-1) \ge j-k-1$$

for $j = k+1, \dots, n$. Thus

$$n|\mathbf{y}|_1 = -\sum_{j=1}^{k} y_j + \sum_{j=k+1}^{n} y_j \ge \sum_{h=0}^{k-1} h + \sum_{h=0}^{n-k-1} h = \frac{(k-1)k}{2} + \frac{(n-k-1)(n-k)}{2}$$
$$\ge \frac{n(n-2)}{4}.$$

□

We can now prove 3). The integers $y_1, \dots, y_n$ are pairwise distinct, since α is a generator of $\mathbb{Q}(\beta_1, \dots, \beta_n)/\mathbb{Q}$. Thus we may assume $y_{j+1} - y_j \ge 1$ for $j = 1, \dots, n-1$. From the lower bound for $M(\alpha)$ in 2) and from the lemma above we get:

$$c_n|\mathbf{y}|_1 \sim \sqrt{\frac{2}{\pi n}}\,|\mathbf{y}|_1 \ge \sqrt{\frac{2}{\pi n}}\,\frac{n-2}{4} \sim \sqrt{\frac{n}{8\pi}}\,.$$

□

4. Proof of Theorem 1.2

The proof of the first assertion of Theorem 1.2 is similar to the proof of the corresponding assertion of Theorem 1.1.

For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ we have

$$|\sigma\alpha| \le |\mathbf{a}|_1 \max\{|\beta_1|, \dots, |\beta_n|\} \le |\mathbf{a}|_1 M(\beta)$$

which shows the upper bound for $M(\alpha)$ in 2). We now prove the lower bound. Let T_n be the set of transposition of $\mathfrak{S}_n$ and, for $\tau = (i,j) \in T_n$, let A_τ be the set of permutation of $\mathfrak{S}_n$ with support $\{1, \dots, n\}\backslash\{i,j\}$ and with no orbits of length 2.

Lemma. *For $n \geq 3$, let Λ_n be the set of permutation of $\mathfrak{S}_n$ with no orbits of length 1 or 2. Then $|\Lambda_n| \geq n!/12$.*

Proof. The inclusion-exclusion principle shows that the set of permutation of $\mathfrak{S}_n$ without fixed points has cardinality

$$\kappa(n) := n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!}.$$

Notice that $1/3 \leq \kappa(n)/n! \leq 1/2$ for $n \geq 3$. Again by the inclusion-exclusion principle

$$|\Lambda_n| \geq \kappa(n) - \frac{n(n-1)}{2}\kappa(n-2) \geq \frac{n!}{3} - \frac{n(n-1)}{2} \cdot \frac{(n-2)!}{2} = \frac{n!}{12}.$$

□

By the lemma above (recall that $n \geq 5$) the sets A_τ have all cardinality $|\Lambda_{n-2}| \geq \frac{(n-2)!}{12}$. Let

$$\Delta = \prod_{\tau \in T_n} \prod_{\sigma \in A_\tau} |\tau\sigma\alpha - \sigma\alpha|.$$

For $\tau = (i,j) \in T_n$ with $1 \leq i < j \leq n$ and $\sigma \in A_\tau$ we have

$$\tau\sigma\alpha - \sigma\alpha = (a_j - a_i)(\beta_i - \beta_j)$$

since the support of σ is disjoint from $\{i,j\}$. Thus

$$\Delta = \Big(|V(\mathbf{a})| \cdot |\mathrm{disc}(\beta)|^{1/2}\Big)^{|\Lambda_{n-2}|}.$$

Let τ, $\tau' \in T_n$ and let $\sigma \in A_\tau$, $\sigma' \in A_\tau$. Then $\tau\sigma \neq \sigma'$ (since the supports of $\tau\sigma$ σ' are not the same). If $\tau = \tau'$ and $\sigma \neq \sigma'$ then $\tau\sigma \neq \tau'\sigma'$ and $\sigma \neq \sigma'$. Moreover, if $\tau \neq \tau'$ then again $\tau\sigma \neq \tau'\sigma'$ (since σ has no orbits of length 2) and $\sigma \neq \sigma'$ (since the supports of σ and $\sigma'$are not the same). Thus

$$\Delta \leq \prod_{\tau \in T_n} \prod_{\sigma \in A_\tau} 2\max(|\tau\sigma\alpha|, 1)\max(|\sigma\alpha|, 1) \leq 2^{|T_n| \cdot |\Lambda_{n-2}|} M(\alpha).$$

From the two last displayed equations and from the inequality $|\Lambda_{n-2}| \geq \frac{(n-2)!}{12}$ we get

$$\begin{aligned} M(\alpha)^{1/n!} &\geq \Big(2^{-|T_n|}|V(\mathbf{a})| \cdot |\mathrm{disc}(\beta)|^{1/2}\Big)^{\frac{|\Lambda_{n-2}|}{n!}} \\ &= 2^{-\frac{1}{24}}\Big(|V(\mathbf{a})| \cdot |\mathrm{disc}(\beta)|^{1/2}\Big)^{\frac{1}{12n(n-1)}}. \end{aligned}$$

We finally prove 3). Notice that the result is trivial if $n \leq 4$, thus we assume $n \geq 5$. The integers $a_1, \ldots, a_n$ are pairwise distinct, since α is a generator of $\mathbb{Q}(\beta_1, \ldots, \beta_n)/\mathbb{Q}$. Thus we may assume $a_{j+1} - a_j \geq 1$ for $j = 1, \ldots, n-1$, which implies

$$|V(\mathbf{a})| = \prod_{i=1}^{n} \prod_{j=i+1}^{n} (a_j - a_i) \geq \prod_{i=1}^{n} \prod_{j=i+1}^{n} (j - i) = \prod_{h=1}^{n} h!.$$

A computation shows that $\prod_{h=1}^{n} h! \geq n^{n(n-1)/4}$. Thus, by 2) and since $|\mathrm{disc}(\beta)| \geq 1$,

$$M(\alpha)^{1/n!} \geq 2^{-\frac{1}{24}} \left(|V(\mathbf{a})| \cdot |\mathrm{disc}(\beta)|^{1/2} \right)^{\frac{1}{12n(n-1)}} \geq (n/4)^{1/48}.$$

□

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, I. Pritsker, C. Smyth and J. Vaaler, "Appendix to Report on BIRS workshop 15w5054 on The Geometry, Algebra and Analysis of Algebraic Numbers: Problems proposed by participants".
   Available at http://www.birs.ca/workshops/2015/15w5054/report15w5054.pdf
4. E. Dobrowolski, "On a question of Lehmer and the number of irreducible factors of a polynomial", *Acta Arith.*, **34** (1979), 391–401.
5. D.H. Lehmer, "Factorization of certain cyclotomic functions"; *Ann. of Math.*, **34** (1933), 461–479.
6. C. J. Smyth, "Additive and Multiplicative Relations Connecting Conjugate Algebraic Numbers", *J. of Number Theory* **23** (1986), 243–254.