Lower bounds for the house in some radical extensions

Francesco Amoroso

Lower bounds for the house in some radical extensions

Francesco Amoroso[(1)]

[(1)] *Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139*
Université de Caen, Campus II, BP 5186
14032 Caen Cedex, France

1 Introduction

Let us consider the infinite extension

$$L = \mathbb{Q}(2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots).$$

Obviously, there exist algebraic numbers α in L of positive but arbitrary small (absolute, logarithmic) Weil's height:

$$h(2^{1/n}) = \frac{1}{n} h(2) = \frac{\log 2}{n}.$$

A very special (but still open) case of a conjecture of Rémond[1] suggests that these are the only exceptions. More precisely, the conjecture predicts in this case that for each $\alpha \in L^*$ we have that either $\alpha = \pm 2^{k/n}$ for some n, $k \in \mathbb{N}$ or $h(\alpha) \geq c$ for some absolute constant $c > 0$. A partial result in this direction was proven in [1], where we give a positive answer when L is replaced by the subfield $\mathbb{Q}(2^{1/3}, 2^{1/3^2}, 2^{1/3^3}, \ldots)$ (the results of *op.cit.* is indeed more general).

Now we restrict ourself to algebraic integers α in L and we consider instead of the height the so-called house of α, that is the maximum modulus $\overline{|\alpha|}$ of its algebraic conjugates. Since

$$h(\alpha) \leq \log \overline{|\alpha|},$$

we expect again to have either $\alpha = \pm 2^{k/n}$ for some n, $k \in \mathbb{N}$ or $\overline{|\alpha|} \geq C$ for some $C > 1$.

Note that lower bounds for the house can be easier to prove than lower bounds for the height, as the following fondamental example shows. Let $\gamma \in \overline{\mathbb{Q}}^*$ be an algebraic integer of degree d, not a root of unity. Lehmer conjecture (1933) predicts

[1] See [10], conjecture 3.4 and [1] for further references.

the lower bound $h(\gamma) \geq c/d$ for some absolute $c > 0$. Schinzel-Zassenhaus conjecture (1965) predicts the lower bound $\overline{|\gamma|} \geq C^{1/d}$ for some absolute $C > 1$. Thus Schinzel-Zassenhaus is a consequence of Lehmer, and for long time it was (wrongly) believed that both are of the same difficulty. In spite of that, Dimitrov [7] recently proved in a very beautiful way Schinzel-Zassenhaus (with $C = 2^{1/4}$) while Lehmer is still open. This may suggest that, even in our setting, lower bounds for the house for integers in L can be more easily proved than lower bounds for the height.

The following is a corollary of our main result.

Corollary 1.1. *Let*[2] $\alpha \in \mathbb{Z}[2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots]$ *be non-zero. Then either* $\alpha = \pm 2^k$ *for some* n, $k \in \mathbb{N}$ *or*

$$\overline{|\alpha|} \geq \sqrt{2}\,.$$

The proof of this statement is easy enough to be sketched in the introduction. Take a non-zero $\alpha \in \mathbb{Z}[2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots]$ outside the multiplicative group generated by ± 1 and by the nth roots of 2. Thus $\alpha \in \mathbb{Z}[2^{1/N}]$ for some positive integer N and we can write $\alpha = a_0 + a_1 2^{1/N} + \cdots + a_{N-1} 2^{(N-1)/N}$ for some integers $a_0, \ldots, a_{N-1}$. We consider the trace $\mathrm{Tr}\colon \mathbb{Q}(2^{1/N}) \to \mathbb{Q}$. Our result rests on this elementary remark:

$$\frac{1}{N}\mathrm{Tr}(2^{j/N}) = \begin{cases} 1 & \text{if } j \equiv 0 \bmod N; \\ 0 & \text{otherwise.} \end{cases}$$

We distinguish two cases.

First case. There exists an index j such that $|a_j| \geq 2$. Since all the conjugates of $2^{-j/N}$ have absolute value $2^{-j/N} \leq 1$ we have:

$$2 \leq |a_j| = \frac{1}{N}|\mathrm{Tr}(2^{-j/N}\alpha)| \leq \overline{|\alpha|}.$$

Thus we get in this case the better lower bound $\overline{|\alpha|} \geq 2$.

Second case. For each j we have $|a_j| \leq 1$. Then, by assumption, there exist two distinct indexes j_0, j_1 such that $a_{j_0} = \pm 1$ and $a_{j_1} = \pm 1$. Choosing the sign in a right way we get

$$\frac{1}{N}|\mathrm{Tr}((2^{-j_0/N} \pm 2^{-j_1/N})\alpha)| = 2.$$

We now prove an upper bound for the quantity on the left hand side. Let $k = N/\gcd(j_1 - j_0, N)$. We notice that $k \geq 2$ since $j_0 \neq j_1$. Thus

$$\frac{1}{N}|\mathrm{Tr}((2^{-j_0/N} + 2^{-j_1/N})\alpha)| \leq \overline{|\alpha|}\frac{1}{k}\sum_{l=0}^{k-1}|2^{-j_0/N} \pm 2^{-j_1/N}\exp(2\pi l i/k)|.$$

[2]Note that $\mathbb{Z}[2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots]$ is not the full ring of integer of L, see Remark 1.2.

We quote the following elementary estimate (see Lemma 2.1 in section 2), which holds since $2^{-j_0/N}$, $2^{-j_1/N} \leq 1$ and $k \geq 2$:

$$\frac{1}{k}\sum_{l=0}^{k-1} |2^{-j_0/N} \pm 2^{-j_1/N}\exp(2\pi l i/k)| \leq \sqrt{2}. \tag{1.1}$$

We get

$$\overline{|\alpha|} \geq 2/\sqrt{2} = \sqrt{2}$$

as required.

Remark 1.2. *The above argument cannot be extended to the full ring of integers, since for arbitrary integers in $\mathbb{Q}(2^{1/N})$ the trace could be 1. Consider the following exemple taken from [6, Theorem 5.1]. Let $p \geq 3$ be a Wieferich prime to base 2, that is a prime satisfying the congruence $2^{p-1} \equiv 1 \bmod p^2$, as for instance $p = 1093$. Then $\gamma = (2^{1/p} - 2)^{p-1}/p \notin \mathbb{Z}[2^{1/p}]$ is an integer of trace 2^{p-1}. Taking a suitable linear combination over $\mathbb{Z}$ of γ and 1, we get an integer $\alpha \in \mathbb{Q}(2^{1/p})$ of trace 1.*

The lower bound $\overline{|\alpha|} \geq \sqrt{2}$ in this corollary holds even replacing the base 2 by any other integral base ≥ 2. Even more, we can consider roots of infinitely many integers, and moreover we can replace $\mathbb{Z}$ by $\mathbb{Z}[\zeta_n]_{n\in\mathbb{N}}$ (with ζ_n a nth root of unity), at the cost of a slight worst lower bound:

Corollary 1.3. *Let $\alpha \in \mathbb{Z}[\zeta_n, p^{1/n}]_{n\in\mathbb{N},\, p \text{ prime}}$ be non-zero. Then either $\alpha^n \in \mathbb{N}$ for some $n \in \mathbb{N}$ or*

$$\overline{|\alpha|} \geq \sqrt{\frac{1+\sqrt{5}}{2}}\,.$$

More generally we have the following statement. Let $K \subset \mathbb{C}$ be a subfield of $\overline{\mathbb{Q}}$, and let $\mathcal{O}$ be a subring of K such that the following holds.

There exists $C > 1$ such that for each non-zero $\gamma \in \mathcal{O}$

$$\text{either } \gamma \text{ is a root of unity, or } \overline{|\gamma|} \geq C. \tag{1.2}$$

Let $\gamma_1, \gamma_2, \ldots \in \mathcal{O}$ be non-zero. We assume that for each j the archimedean absolute value of γ_j is ≥ 1. We further assume that for each finite subset $\Gamma \subset \{\gamma_1, \gamma_2, \ldots\}$ and for each $N \in \mathbb{N}$ the extension $K(\gamma^{1/N} | \gamma \in \Gamma)/K$ is of degree $N^{|\Gamma|}$.

Remark 1.4. *By Kummer's Theory this last assertion holds if*

i) K contains the roots of unity;

ii) None of the γ_j is a (non trivial) power in K;

iii) For each $N \in \mathbb{N}$, $\gamma_1, \gamma_2, \ldots$ are multiplicatively independent modulo[3] $(K^*)^N$.

[3]That is: $\gamma_1^{a_1}, \ldots, \gamma_r^{a_r} \in (K^*)^N$ whenever $\gamma_1^{a_1} \cdots \gamma_r^{a_r} \in (K^*)^N$ for some integers a_i.

The following is our main result.

Theorem 1.5. *Let $\alpha \in \mathcal{O}[\gamma_i^{1/n}]_{i,n\in\mathbb{N}}$ be non-zero. Then either $\alpha^n = \gamma_1^{k_1}\cdots\gamma_r^{k_r}$ for some $n, r, k_1, \ldots, k_r \in \mathbb{N}$ or*

$$\overline{|\alpha|} \geq \min(C, \sqrt{2}) \ .$$

More precisely, if $\overline{|\alpha|} < C$ then the maximum absolute value of the conjugates of α over K is $\geq \sqrt{2}$.

The plan of the paper is as follow. In section 2, Lemma 2.1, we prove a L_1-mean estimate which implies 1.1. In section 3 we prove Theorem 1.5 and we deduce Corollary 1.3 from it. We conclude this article with a more speculative section 4 where we state some questions and remarks on lower bounds for the house.

Acknowledgment. We are indebted with Gaël Rémond, who suggests us a simple proof of Lemma 2.1 with a better (and optimal) constant, and with Lukas Pottmeyer for the Remark 4.2.

2 An elementary lemma

In this section we prove the following elementary lemma. Inequality (1.1) in the introduction is a special case.

Lemma 2.1. *Let x, y be non-zero complex numbers and let $k \geq 2$ be an integer. Then*

$$\frac{1}{k}\sum_{l=0}^{k-1} |x + y\exp(2\pi l i/k)| \leq \sqrt{x^2+y^2} \ .$$

Proof. By Cauchy-Schwartz,

$$\frac{1}{k}\sum_{l=0}^{k-1} |x + y\exp(2\pi l i/k)| \leq \frac{1}{k}\left(\sum_{l=0}^{k-1} |x + y\exp(2\pi l i/k)|^2\right)^{1/2} \times \sqrt{k} \ .$$

Writing $y/x = |y/x|\exp(i\theta)$ we get

$$|x + y\exp(it)|^2 = |x|^2 + 2|xy|\cos(\theta + t) + |y|^2.$$

Remark that $\sum_{l=0}^{k-1}\exp(2\pi l i/k) = 0$ since $k \geq 2$. Hence $\sum_{l=0}^{k-1}\cos(\theta + 2\pi l i/k) = 0$ and

$$\sum_{l=0}^{k-1} |x + y\exp(2\pi l i/k)|^2 = k(|x|^2 + |y|^2).$$

The conclusion follows. □

Remark 2.2. *The result is optimal: take $x/y = i$ and $k = 2$.*

3 Proofs of the main results

Proof of Theorem 1.5 The proof follows the same lines as the proof sketched in the introduction. Take a non-zero $\alpha \in \mathcal{O}[\gamma_i^{1/n}]_{i,n\in\mathbb{N}}$. Thus $\alpha \in \mathcal{O}[\gamma_1^{1/N}, \dots, \gamma_r^{1/N}]$ for some r, $N \in \mathbb{N}$. Let $L = K(\gamma_1^{1/N}, \dots, \gamma_r^{1/N})$ and $\mathrm{Tr} = \mathrm{Tr}_K^L$ be the trace relative to K. We suppose that for each $n, k_1, \dots, k_r \in \mathbb{N}$, α does not satisfy $\alpha^n = \gamma_1^{k_1} \cdots \gamma_r^{k_1}$. We write

$$\alpha = \sum_{\mathbf{j}} a_{\mathbf{j}} \gamma_1^{j_1/N} \cdots \gamma_r^{j_r/N}.$$

where the sum is over the multi-indeces $\mathbf{j} = (j_1, \dots, j_r)$ with $0 \le j_i < N$. We distinguish two cases.

First case. There exists an index $\mathbf{j}$ such that $a_{\mathbf{j}}$ is neither zero nor a root of unity. We have

$$\frac{1}{N^r}\mathrm{Tr}(\gamma^{-j_1/N} \cdots \gamma^{-j_r/N}\alpha) = a_{\mathbf{j}}.$$

By assumption (1.2), $\overline{|a_{\mathbf{j}}|} \ge C$. Thus

$$C \le \overline{|a_{\mathbf{j}}|} = \frac{1}{N^r}\overline{|\mathrm{Tr}(\gamma^{-j_1/N} \cdots \gamma^{-j_r/N}\alpha)|} \le \overline{|\alpha|}$$

since all the conjugates of $\gamma^{-j/N}$ have absolute value ≤ 1. We get in this case the lower bound $\overline{|\alpha|} \ge C$.

Second case. For each $\mathbf{j}$ the coefficient $a_{\mathbf{j}}$ is either zero or a root of unity. By assumption, there exist two distinct multi-indexes $\mathbf{j}$, $\mathbf{j}'$ such that $a_{\mathbf{j}}$ and $a_{\mathbf{j}'}$ are both roots of unity. Otherwise, $\alpha = a_{\mathbf{j}}\gamma_1^{j_1/N} \cdots \gamma_r^{j_r/N}$ for some $\mathbf{j}$ and in this case either $\alpha = 0$ or $\alpha^{Nk} = \gamma_1^{j_1 k} \cdots \gamma_r^{j_r k}$ if $a_{\mathbf{j}}$ is a kth root of unity.

Let $x = (a_{\mathbf{j}}\gamma_1^{j_1/N} \cdots \gamma_r^{j_r/N})^{-1}$ and $y = (a_{\mathbf{j}'}\gamma_1^{j_1'/N} \cdots \gamma_r^{j_r'/N})^{-1}$. Then

$$\frac{1}{N^r}\mathrm{Tr}((x+y)\alpha) = 2. \tag{3.1}$$

By assumption L/K is of degree N^r. Thus the K-embeddings $L \hookrightarrow \mathbb{C}$ are given by $\sigma_{\boldsymbol{\omega}}(\gamma_i^{1/N}) = \omega_i \gamma_i^{1/N}$ with $\omega_i \in \boldsymbol{\mu}_N$, the group of Nth roots of unity. Thus

$$\begin{aligned}
\frac{1}{N^r}|\mathrm{Tr}((x+y)\alpha)| &= \frac{1}{N^r}\Big|\sum_{\boldsymbol{\omega}\in\boldsymbol{\mu}_N^r}(\sigma_{\boldsymbol{\omega}}(x) + \sigma_{\boldsymbol{\omega}}(x))\sigma_{\boldsymbol{\omega}}(\alpha)\Big| \\
&\le \overline{|\alpha|}_K \frac{1}{N^r}\sum_{\boldsymbol{\omega}\in\boldsymbol{\mu}_N^r}|x + \omega_1^{j_1'-j_1} \cdots \omega_r^{j_r'-j_r} y| \\
&= \overline{|\alpha|}_K \frac{1}{k}\sum_{\boldsymbol{\omega}\in\boldsymbol{\mu}_k}|x + \omega_k y|
\end{aligned}$$

with

$$k = \operatorname{lcm}\left(\frac{N}{\gcd(j_1' - j_1, N)}, \ldots, \frac{N}{\gcd(j_1' - j_1, N)}\right).$$

and where

$$\overline{|\alpha|}_K = \max\{|\sigma\alpha|,\ \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)\} \leq \overline{|\alpha|}$$

is the maximum of the absolute value of the conjugates of α over K.

Note that $k \geq 2$ since for at least one of the index i we have $j_i' \not\equiv j_i \bmod N$. Note also that $|x|$, $|y| \leq 1$ (since $|\gamma_j| \geq 1$). Thus we can apply Lemma 2.1:

$$\frac{1}{N^r}|\mathrm{Tr}((x+y)\alpha)| \leq \sqrt{2} \times \overline{|\alpha|}. \tag{3.2}$$

By (3.1) and (3.2) we get the desired conclusion.

□

Proof of Corollary 1.3 We apply Theorem 1.5, choosing $K = \mathbb{Q}^{\mathrm{ab}}$ the maximal cyclotomic extension and $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\zeta_n]_{n\in\mathbb{N}}$. Then (1.2) holds with

$$C = \sqrt{\frac{1+\sqrt{5}}{2}} < \sqrt{2}$$

by a result of Schinzel (apply [11], Corollary 1′, p. 386, to the linear polynomial $P(z) = z - \alpha$; see the next section for details). Notice also that the square of the integers are in K. We choose $\gamma_i = \sqrt{p_i}$ where $(p_i)_{i\in\mathbb{N}}$ is the sequence of the rational primes. We still have to show that for each finite subset $\Gamma \subset \{\gamma_1, \gamma_2, \ldots\}$ and for each $N \in \mathbb{N}$ the extension $K(\gamma^{1/N} | \gamma \in \Gamma)/K$ is of degree $N^{|\Gamma|}$.

We make use of Remark 1.4. Assertion i) is satisfied by the choice of K; and assertion ii) is satisfied since K^* does not contain nontrivial kth roots of rationals for $k \geq 3$ (they generate over $\mathbb{Q}$ a non-Galois extension). It is thus enough to prove assertion iii), *i.e.* that $\gamma_1, \gamma_2, \ldots$ are multiplicatively independent modulo $(K^*)^N$. Let $\alpha := \prod_p p^{a_p/2}$ where the product is over a finite set of primes and where a_p are integers. Suppose $\alpha \in (K^*)^N$ for some $N \geq 2$. Then $\alpha^2 \in (K^*)^{2N} \cap \mathbb{Q}^*$. Since K^* does not contains nontrivial kth roots of rationals for $k \geq 3$, $\alpha^2 \in (\mathbb{Q}^*)^N$ which in turns imply $n \mid a_p$ for all p, and thus $p^{a_p/2} \in (K^*)^N$.

□

4 Concluding remarks

Dimitrov's proof of Schinzel-Zassenhaus conjecture and our results in this paper suggest that lower bounds for the house are sensibly simpler to prove than lower bound for the height. This opens a large spectre of conjectures, problems and

results by considering the house of an algebraic number instead of the more familiar Weil's height.

Let $\mathcal{A}$ be a set of algebraic numbers. Following [5], we say that $\mathcal{A}$ has the *Bogomolov Property* (B) if there exists a real number $c = c(\mathcal{A}) > 0$ such that the set of non-zero $\alpha \in \mathcal{A}$ of height $< c$ consists of roots of unity. Several examples of fields with property (B) are known. For instance the field $\mathbb{Q}^{\mathrm{tr}}$ of all totally real algebraic numbers ([11]), the fields with bounded local degrees at some finite place ([5]), the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ ([3]). We refer the interested reader to the introduction of [2] for details and for other examples.

Property (B) for fields is not stable by finite extensions. For instance[4] the field $\mathbb{Q}^{\mathrm{tr}}(i)$, which is the compositum of all CM-field, does not have property (B), see again [2], section 5. However, the ring of integers of $\mathbb{Q}^{\mathrm{tr}}(i)$ has property (B) by a result of Schinzel (apply [11], Corollary $1'$, p. 386, to the linear polynomial $P(z) = z - \alpha$), and the same is true for any finite extension of $\mathbb{Q}^{\mathrm{tr}}$ by [9], Theorem 1. Since $h(\alpha) \leq \log \overline{|\alpha|}$, *a fortiori* this ring satisfies the *House Property* below:

Definition 4.1. *Let $\mathcal{A}$ be a set of algebraic integers. We say that $\mathcal{A}$ has the House Property if there exists a real number $C = C(\mathcal{A}) > 1$ such that the set of non-zero $\alpha \in \mathcal{A}$ of house $< C$ consists of roots of unity.*

By abuse of notation we say that a field of algebraic numbers has the House Property if its ring of integers have it. In this context, some questions arise naturally.

By the remark above, fields with (B) satisfy the House Property, and moreover this property is satisfied by $\mathbb{Q}^{\mathrm{tr}}(i)$, which does not satisfy (B). Are there other significant examples of fields which satisfy the House Property but do not have (B), or at least for which we cannot prove that they satisfy (B)?

Related to this question, we might ask if the House Property is stable by finite extensions. A positive answer could be suggested by the example $\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}^{\mathrm{tr}}$ above, where the House Property is satisfied even if $\mathbb{Q}^{\mathrm{tr}}(i)$ does not satisfy (B). In spite of that we have:

Remark 4.2 (Pottmeyer)**.** *Let α be any Salem number*[5] *and $K = \mathbb{Q}(\alpha)$. Let β be any non-real conjugate of α. Then $\beta^{1/n} \in K^{\mathrm{tr}}(i)$ for each $n \in \mathbb{N}$. In particular, $K^{\mathrm{tr}}(i)$ does not satisfy the House Property.*

Proof. Let $n \in \mathbb{N}$. Then all Galois conjugates of $\beta^{1/n}$ over K have absolute value 1. By [9, Lemma 1], $\beta^{1/n} \in K^{\mathrm{tr}}(i)$. □

By the already quoted result of Schinzel, K^{tr} satisfies (B) and hence the House property. Thus $K^{\mathrm{tr}}(i)/K^{\mathrm{tr}}$ is a degree two extension which does not satisfy the House property even if the ground field does.

[4]note that the extension $\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}^{\mathrm{tr}}$ is essentially the only known example of this phenomenon, see [9].

[5]Thus $\alpha > 1$ is an algebraic integer, α^{-1} is a conjugate of α, and the other conjugates lie on the unit circle.

References

[1] F. Amoroso, "On a conjecture of G. Rémond." *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* **15** (2016), 599–608.

[2] F. Amoroso, S. David and U. Zannier, "On fields with the property (B)", *Proc. Amer. Math. Soc.*, **142** n° 6, pages 893–1910, 2014.

[3] F. Amoroso and R. Dvornicich, "A Lower Bound for the Height in Abelian Extensions." *J. Number Theory* **80** (2000), no 2, 260–272.

[4] F. Amoroso and U. Zannier, "A relative Dobrowolski's lower bound over abelian extensions." *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **29** (2000), no. 3, 711–727.

[5] E. Bombieri and U. Zannier, "A note on heights in certain infinite extensions of $\mathbb{Q}$." *Rend. Mat. Acc. Lincei (9)*, **12** (2001), 5–14.

[6] K. Conrad, "The ring of integers in a radical extension". `https://kconrad.math.uconn.edu/blurbs/gradnumthy/integersradical.pdf`.

[7] V. Dimitrov, "A proof of the Schinzel-Zassenhaus conjecture on polynomials". Preprint. `https://arxiv.org/abs/1912.12545`

[8] E. Dobrowolski, "On the maximal modulus of conjugates of an algebraic integer. " *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **26** (1978), 291–292.

[9] L. Pottmeyer, "A note on extensions of $\mathbb{Q}^{\mathrm{tr}}$". *J. Théor. Nombres Bordeaux* **28** (2016), 735–742.

[10] G. Rémond, "Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink". Panor. Synthèses, 52, Soc. Math. France, Paris, 2017.

[11] A. Schinzel, "On the product of the conjugates outside the unit circle of an algebraic number"; Acta Arith. **24** (1973), 385–399. Addendum; ibid., **26** (1973), 329–361.