LOWER BOUNDS FOR THE HEIGHT IN GALOIS EXTENSIONS

F. AMOROSO AND D. MASSER

Abstract: We prove close to sharp lower bounds for the height of an algebraic number in a Galois extension of $\mathbb{Q}$.

1. Introduction

For an algebraic number α of degree d denote by $h(\alpha) \geq 0$ the absolute logarithmic Weil height, that is

$$h(\alpha) = \frac{1}{d}\left(\log |a| + \sum_i \max\{\log |\alpha_i|, 0\}\right),$$

where a is the leading coefficient of a minimal equation over $\mathbb{Z}$ for α and α_i are its algebraic conjugates. Recall that $h(\alpha) = 0$ if and only if $\alpha = 0$ or α is a root of unity. The well-known Lehmer Problem from 1933 asks whether there is a positive constant c such that

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

whenever $\alpha \neq 0$ has degree d and is not a root of unity. This is still unsolved, but the celebrated result of Dobrowolski [7] implies that for any $\varepsilon > 0$ there is $c(\varepsilon) > 0$ such that $h(\alpha) \geq c(\varepsilon)d^{-1-\varepsilon}$ (we will not worry about logarithmic refinements in this note).

The inequality in the Lehmer Problem has been established for various classes of α. Thus Breusch [5] proved it for non-reciprocal α, in particular whenever d is odd (see also Smyth [14] for the best possible constant), and David with the first author [1, *Corollaire* 1.7] proved it when $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension. See also their *Corollaire 1.8* for a generalization to extensions that are "almost Galois".

In this note we improve the result in the Galois case, and we even show that for any $\varepsilon > 0$ there is $c(\varepsilon) > 0$ such that

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

when $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension. This is related to a problem posed by Smyth during a recent BIRS workshop (see [12, problem 21, p. 17]), who asks for small positive values of $h(\alpha)$ for $\alpha \in \overline{\mathbb{Q}}$ with $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois.

2. Auxiliary results

We start with a lower bound for the height which is crucial in the proof of the next section.

Theorem 2.1. *Let $K/\mathbb{Q}$ be an abelian extension and let $\alpha_1, \ldots, \alpha_r$ be multiplicatively independent algebraic numbers. Then for any $\varepsilon > 0$ there exists $C(\varepsilon) > 0$ such that*

$$\max_i h(\alpha_i) \geq C(\varepsilon)D^{-1/r-\varepsilon}$$

Date: August 3, 2016.

where $D = [K(\alpha_1, \dots, \alpha_r) : K]$.

This deep result (which we have stated in a simplified form) was proved in several steps. In the special cases $K = \mathbb{Q}$ and $r = 1$, it is the main result of [1] and [3] respectively. The general case (see [6]) was the object of the Ph.D. Thesis of E. Delsinne, under the supervision of the first author.

We now state a result whose proof is implicit in [1, *Corollaire* 6.1].

Lemma 2.2. *Let $F/\mathbb{Q}$ be a Galois extension and $\alpha \in F^\times$. Let ρ be the multiplicative rank of the conjugates $\alpha_1, \dots, \alpha_d$ of α over $\mathbb{Q}$, and suppose $\rho \geq 1$. Then there exists a subfield $L \subseteq F$ which is Galois over $\mathbb{Q}$ of degree $[L : \mathbb{Q}] = n \leq n(\rho)$ and an integer $e \geq 1$ such that $\mathbb{Q}(\zeta_e) \subseteq F$ (for a primitive eth root of unity ζ_e) and $\alpha^e \in L$.*

Proof. Let e be the order of the group of roots of unity in F, so that F contains $\mathbb{Q}(\zeta_e)$. Define $\beta_i = \alpha_i^e$ $(i = 1, \dots, d)$ and $L = \mathbb{Q}(\beta_1, \dots, \beta_d)$. The $\mathbb{Z}$-module

$$\mathcal{M} = \{\beta_1^{a_1} \cdots \beta_d^{a_d} \mid a_1, \dots, a_d \in \mathbb{Z}\}$$

is torsion free (by the choice of e) and so, by the Classification Theorem for abelian groups, is free, of rank ρ. This shows that the action of $\mathrm{Gal}(L/\mathbb{Q})$ over $\mathcal{M}$ defines an injective representation $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_\rho(\mathbb{Z})$. Thus $\mathrm{Gal}(L/\mathbb{Q})$ identifies to a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Z})$. But, by well-known results (see Remark 2.3 below), the cardinalities of the finite subgroups of $\mathrm{GL}_\rho(\mathbb{Z})$ are uniformly bounded by, say, $n = n(\rho)$.

□

Remark 2.3. To quickly see that the order of a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Z})$ is uniformly bounded by some $n(\rho) < \infty$, apply Serre's result [13] which asserts that the reduction mod 3 is injective on the finite subgroups of $\mathrm{GL}_\rho(\mathbb{Z})$. This gives the bound $n(\rho) \leq 3^{\rho^2}$. More precise results are known. Feit [8] (unpublished) shows that the orthogonal group $O_\rho(\mathbb{Z})$ (of order $2^\rho \rho!$) has maximal order for $\rho = 1, 3, 5$ and for $\rho > 10$. For the seven remaining values of ρ, Feit characterizes the corresponding maximal groups. See [9] for more details and for a proof of the weaker statement $n(\rho) \leq 2^\rho \rho!$ for large ρ.

We finally recall a well-known estimate on the Euler's totient function $\phi(\cdot)$ (see for instance [10, Theorem 328, p.267]):

$$\liminf_{n \to \infty} \frac{\phi(n) \log \log n}{n} = e^{-\gamma}. \tag{2.1}$$

3. Main results

We now state two results about α which merely lie in Galois extensions, so are not necessarily generators.

Theorem 3.1. *For any integer $r \geq 1$ and any $\varepsilon > 0$ there is a positive effective constant $c(r, \varepsilon)$ with the following property. Let $F/\mathbb{Q}$ be a Galois extension of degree D and $\alpha \in F^\times$. We assume that there are r conjugates of α over $\mathbb{Q}$ which are multiplicatively independent (so that α is not a root of unity). Then*

$$h(\alpha) \geq c(r, \varepsilon) D^{-1/(r+1) - \varepsilon}.$$

Proof. The new ingredient with respect to *Corollaire 1.7* of [1] is the main result of Delsinne [6], which was not available at that time. We use standard abbreviations like $\ll_\varepsilon, \gg_{r,\varepsilon}$.

Let $\alpha_1, \ldots, \alpha_d$ (with $d \le D$) be the conjugates of α over $\mathbb{Q}$ (so that they lie in F). Their multiplicative rank is at least r. If it is strictly bigger, then Theorem 2.1 (with $K = \mathbb{Q}$) applied to $r+1$ independent conjugates gives

$$h(\alpha) \gg_{r,\varepsilon} D^{-1/(r+1)-\varepsilon} .$$

Thus we may assume that the rank is exactly r.

By Lemma 2.2 there exists a number field $L \subseteq F$ of degree $[L : \mathbb{Q}] = n \le n(r)$ and an integer $e \ge 1$ such that $\mathbb{Q}(\zeta_e) \subseteq F$ and $\alpha^e \in L$.

Now let $\varepsilon > 0$. Since $\alpha^e \in L$ and $[L : \mathbb{Q}] \le n$,

$$h(\alpha) = \frac{1}{e} h(\alpha^e) \gg_r \frac{1}{e}. \tag{3.1}$$

On the other hand, the degree of F over the cyclotomic extension $\mathbb{Q}(\zeta_e)$ is $D/\phi(e)$ and $\alpha_1, \ldots, \alpha_r \in F$ are multiplicatively independent. By Theorem 2.1 (with $K = \mathbb{Q}(\zeta_e)$) we have

$$h(\alpha) \gg_{r,\varepsilon} (D/\phi(e))^{-1/r-\varepsilon} \gg_{r,\varepsilon} e^{1/r} D^{-1/r-\varepsilon} \tag{3.2}$$

(use (2.1)). Combining (3.1) and (3.2) we get

$$h(\alpha)^{r+1} = h(\alpha) h(\alpha)^r \gg_{r,\varepsilon} D^{-1-r\varepsilon}.$$

□

Taking $r = 1$ we get

Corollary 3.2. *For any $\varepsilon > 0$ there is a positive effective constant $c(\varepsilon)$ with the following property. Let $F/\mathbb{Q}$ be a Galois extension of degree D. Then for any $\alpha \in F^\times$ which is not a root of unity we have*

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

For a direct proof of this corollary, which uses [3] instead of the deeper result of [6], see [11, exercise 16.23].

We remark that Corollary 3.2 is optimal: take for F the splitting field of $x^d - 2$, with $D = d\phi(d)$, and $\alpha = 2^{1/d}$. Nevertheless, as mentioned above, this result can be strengthened for a *generator* α of a Galois extension.

Theorem 3.3. *For any $\varepsilon > 0$ there is a positive effective constant $c(\varepsilon)$ with the following property. Let $\alpha \in \overline{\mathbb{Q}}^\times$ be of degree d, not a root of unity, such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Then we have*

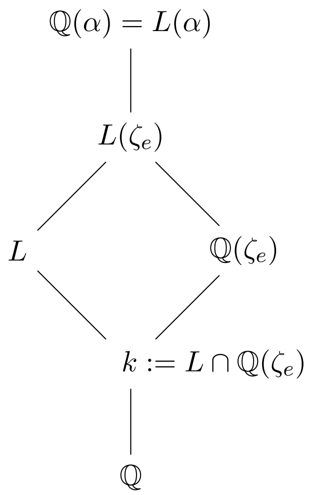
$$h(\alpha) \ge c(\varepsilon) d^{-\varepsilon} .$$

Proof. Let r be the smallest integer $> 1/\varepsilon$. If $r \ge d$ then $d \le 1 + 1/\varepsilon$ and $h(\alpha) \gg_\varepsilon 1$. So we can assume $r < d$. If r among the conjugates of α are multiplicatively independent, by Theorem 2.1 (with $K = \mathbb{Q}$) we have

$$h(\alpha) \gg_\varepsilon d^{-1/r-\varepsilon} \gg_\varepsilon d^{-2\varepsilon} .$$

Otherwise, the multiplicative rank $\rho \ge 1$ of the conjugates of α is at most $r - 1 \le 1/\varepsilon$. By Lemma 2.2 there exists a number field $L \subseteq \mathbb{Q}(\alpha)$ of degree $[L : \mathbb{Q}] = n \le$

$n(\varepsilon)$ and an integer $e \geq 1$ such that $\mathbb{Q}(\zeta_e) \subseteq \mathbb{Q}(\alpha)$ and $\alpha^e \in L$. As a consequence $L(\alpha)/L$ is of degree $e' \leq e$. The diagram



shows that the degree of α over $\mathbb{Q}(\zeta_e)$ is

$$[\mathbb{Q}(\alpha) : L(\zeta_e)] \cdot [L(\zeta_e) : \mathbb{Q}(\zeta_e)] = e' \frac{[L(\zeta_e) : \mathbb{Q}(\zeta_e)]}{[L(\zeta_e) : L]}$$

which is

$$e' \frac{[L : k]}{[\mathbb{Q}(\zeta_e) : k]} = e' \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\zeta_e) : \mathbb{Q}]} = \frac{e'}{\phi(e)} n \leq \frac{e}{\phi(e)} n \ll_\varepsilon d^\varepsilon$$

(use $\phi(e) \leq d$ and (2.1)). By Theorem 2.1 (with $K = \mathbb{Q}(\zeta_e)$ and $r = 1$) we get

$$h(\alpha) \gg_\varepsilon d^{-2\varepsilon} .$$

□

We note that Theorem 3.3 is nearly best possible in the sense that an inequality $h(\alpha) \gg d^\delta$ would be false for any fixed $\delta > 0$. For example for $\alpha = 1 + \zeta_e$ with $d = \phi(e)$ one has $h(\alpha) \leq \log 2$. Or $\alpha = 2^{1/e} + \zeta_e$, whose degree is easily seen to be $e\phi(e)$, with $h(\alpha) \leq 2 \log 2$. But Smyth in [12] quoted above asked whether even $h(\alpha) \gg 1$ is true, a kind of "Galois-Lehmer Problem". We do not know, but it would imply the main result of Amoroso-Dvornicich [2] on abelian extensions, and a slightly weaker result of Amoroso-Zannier [4, Corollary 1.3] on dihedral extensions.

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), no 2, 260–272.
3. 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.
4. F. Amoroso and U. Zannier, "A uniform relative Dobrowolski's lower bound over abelian extensions". *Bull. London Math. Soc.*, **42** (2010), no. 3, 489–498.
5. R. Breusch, "On the distribution of the roots of a polynomial with integral coefficients", *Proc. Amer. Math. Soc.* **2** (1951), 939–941.

6. E. Delsinne, "Le problème de Lehmer relatif en dimension supérieure", *Ann. Sci. École Norm. Sup.* **42**, fascicule 6 (2009), 981–1028.
7. E. Dobrowolski, "On a question of Lehmer and the number of irreducible factors of a polynomial", *Acta Arith.*, **34** (1979), 391–401.
8. W. Feit, "The orders of finite linear groups". Preprint 1995.
9. S. Friedland, "The maximal orders of finite subgroups in $\mathrm{GL}_n(\mathbb{Q})$", Proc. Amer. Math. Soc. **125** (1997), 3519–3526.
10. G. H. Hardy and E. M. Wright, "An introduction to the theory of numbers". Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979. xvi+426 pp.
11. D. Masser, "Auxiliary Polynomials in Number Theory". In Press.
12. 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
13. J-P. Serre. "Rigidité du foncteur de Jacobi d'échelon $n \geq 3$". Appendice à l'exposé 17 du séminaire Cartan, 1960-1961.
14. C. J. Smyth, "On the product of the conjugates outside the unit circle of an algebraic number", *Bull. London Math. Soc.* **3** (1971), 169–175.