Explicit lower bounds for the height in Galois extensions of number fields

Jonathan Jenvrin

Explicit lower bounds for the height in Galois extensions of number fields *

Jonathan Jenvrin

Abstract

Amoroso and Masser proved that for every real $\epsilon > 0$, there is a constant $c(\epsilon) > 0$, with the property that, for every algebraic number α such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension, the height of α is either 0 or at least $c(\epsilon)[\mathbb{Q}(\alpha) : \mathbb{Q}]^{-\epsilon}$. In this article, we establish an explicit version of this theorem.

1 Introduction

In this article, we let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$. For an algebraic number α, we denote by $h(\alpha) \geq 0$ its absolute logarithmic Weil height.

It's well know by Kronecker's theorem that $h(\alpha) = 0$ if and only if $\alpha = 0$ or α is a root of unity. Lehmer's conjecture predicts the existence of a positive constant c such that

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

whenever $\alpha \neq 0$ has degree d over $\mathbb{Q}$ and is not a root of unity.

This is obviously true for α not a unit with $c = \log(2)$. The conjecture has been established for various classes of α. For α non-reciprocal (which is always the case for d odd) the result holds true with $c = 3h(\theta) = \log(\theta)$, where θ is the real root > 1 of $X^3 - X - 1$ (see [Sch73]). If α belongs to an abelian extension and $h(\alpha) \neq 0$, we have $h(\alpha) \geq \frac{\log(5)}{12}$ (see [AD00]). For α in a CM-field with $|\alpha| \neq 1$, we have $h(\alpha) \geq \frac{1}{2}\log(\frac{1+\sqrt{5}}{2})$ (see [Sch73]). The best unconditional result we have to Lehmer's conjecture is Dobrowolski's result

*This work has been partially supported by the Institut Fourier, Université Grenoble1, UMR 5582 duCNRS, 100 rue des mathématiques, BP 74, 38402 St Martin d'hères.

[Dob79], which implies that for any $\epsilon > 0$, there is $c(\epsilon) > 0$ such that either $h(\alpha) = 0$ or $h(\alpha) \geq c(\epsilon)d^{-1-\epsilon}$.

Amoroso and David proved Lehmer's conjecture when $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension, see [AD99, Corollaire 1.7]. Later, Amoroso and Masser [AM16] proved the following stronger result.

Theorem 1.1. *For any $\epsilon > 0$, there is a positive effective constant $c(\epsilon)$ with the following property. If $\alpha \in \overline{\mathbb{Q}}^*$ is of degree d over $\mathbb{Q}$, α is not a root of unity and $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, then*

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

The goal of our article is to give a explicit version of this theorem. Our main result is the following:

Theorem 1.2. *Suppose $\alpha \in \overline{\mathbb{Q}}^*$ is of degree d over $\mathbb{Q}$. If α is not a root of unity and $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, then*

$$h(\alpha) \geq \exp\left(-500\log(3d)^{3/4}\log(\log(3d))\right).$$

Theorem 1.2 is proved in Section 3. Our proof strategy relies on that of Amoroso and Masser in [AM16, Theorem 3.3]. There will be two cases. They are related to the comparison of the multiplicative rank ρ of the conjugates of α, and d. If ρ is big in terms of d, then they originally use the main result of [AD99]. It says that for any $\alpha_1, \ldots, \alpha_r$ multiplicatively independent algebraic number and any $\epsilon > 0$, there exists $C(\epsilon)$ such that

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

where $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_r) : \mathbb{Q}]$. We will instead use a more precise and explicit result from [AV12] (see Theorem 2.1). If ρ is small in terms of d, then they use the relative Dobrowolski lower bound of [AZ10]. Again, we will instead apply a more precise and explicit result from [AD07] (see Theorem 2.2). We moreover need an explicit estimate for the Euler Totient function (see Lemma 2.2).

2 Auxiliary Results

We state two important results that will be the key ingredients in our proof. The first was proved by Amoroso and Viada in [AV12, Corollary 1.6], where,

more generally, they give an explicit version of a generalized Dobrowolski result on Lehmer's problem.

Theorem 2.1 ([AV12, Corollary 1.6]). *Let $\alpha_1, \dots, \alpha_n$ be multiplicatively independent algebraic numbers in a number field K. Then*

$$h(\alpha_1) \dots h(\alpha_n) \geq [K : \mathbb{Q}]^{-1} (1050 n^5 \log(3[K : \mathbb{Q}]))^{-n^2(n+1)^2}.$$

The second result was proved by Amoroso and Delsinne in [AD07, Théorème 1.3]. We recall a special case of this theorem, which is enough for our purposes.

Theorem 2.2 ([AD07, Théorème 1.3]). *Let $\alpha \in \overline{\mathbb{Q}}^*$ be not a root of unity and let L be a number field. Then if $L/\mathbb{Q}$ is a finite abelian extension and $D = [L(\alpha) : L]$, we have*

$$h(\alpha) \geq D^{-1} \frac{\log \log(5D)^3}{\log(2D)^4}.$$

The following lemma is a general version of [AM16, Lemma 2.2], with an improvement on the value of $n(\rho)$.

Lemma 2.1. *Let F/K be a finite Galois extension and $\alpha \in F \setminus \{0\}$. Let ρ be the multiplicative rank of the conjugates $\alpha_1, ..., \alpha_d$ of α over K, and suppose $\rho \geq 1$. Then there exists a subfield $L \subset F$ which is Galois over K of degree $[L : K] \leq n(\rho)$ and an integer $k \geq 1$, such that F contains a primitive k-th root of unity ζ_k and $\alpha^k \in L$. We can take*

$$n(\rho) = \rho! 2^\rho \text{ for } \rho = 1, 3, 5 \text{ and } \rho > 10.$$

Otherwise we can take

$$n(\rho) = 135 \rho! 2^{\rho - 1}.$$

Proof. Let k be the order of the group of roots of unity in F, in particular F contains $K(\zeta_k)$. Define $\beta_i = \alpha_i^k$ for $1 \leq i \leq d$ and $L = K(\beta_1, \dots, \beta_d)$. We have $L \subset F$ because F/K is Galois, and we easily check that L/K is Galois. The $\mathbb{Z}-$module

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

is torsion free by the choice of k and so, by the Classification Theorem for abelian group, is free, of rank ρ. This shows that the action of Gal(L/K)

over M defines an injective representation from Gal(L/K) to $\mathrm{GL}_\rho(\mathbb{Z})$, hence Gal(L/K) identifies with a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Z})$. To conclude, we use a theorem stated by Feit in 1996, and proved by Rémond in [Rém20, Théorème 7.1], which, in particular, gives an explicit bound for the order of the maximal finite subgroups of $\mathrm{GL}_\rho(\mathbb{Z})$. □

We end this section with the following two lemmas.

Lemma 2.2. *Let ϕ be the Euler's totient function. For every positive integer n, we have* [1]

$$\frac{n}{\phi(n)} \leq \frac{3\log(\log(3n))}{2\log(\log(3))}$$

and

$$\phi(n) \geq \sqrt{\frac{n}{2}}.$$

Proof. For $n \geq 3$, let

$$a_n = \frac{\phi(n)\log(\log(n))}{n}.$$

We are going to show that $a_n \geq a_3$ for all $n \geq 3$. It's easy to check that $a_4 \geq a_3$, so we can suppose $n \geq 5$. We have (see [BS96, Theorem 8.8.7]) that for $k \geq 3$

$$\phi(k) > \frac{k}{e^\gamma \log(\log(k)) + \frac{3}{\log(\log(k))}}$$

where γ is the Euler's constant. Thus for all $k \geq 3$ we have

$$a_k \geq \frac{\log(\log(k))}{e^\gamma \log(\log(k)) + \frac{3}{\log(\log(k))}}.$$

Consider the function

$$f(x) = \frac{\log(\log(x))}{e^\gamma \log(\log(x)) + \frac{3}{\log(\log(x))}}.$$

Its derivative is

$$f'(x) = \frac{6\log(\log(x))}{x\log(x)(e^\gamma(\log(\log(x)))^2 + 3)^2}.$$

[1] The factor 3 in $\log(\log(3n))$ is here for the cases $n = 1$ and $n = 2$.

So the function f is increasing on the interval $[3, +\infty[$. We can check that $f(5) \geq \frac{2\log(\log(3))}{3}$. As a result, for $n \geq 5$

$$a_n \geq f(n) \geq f(5) \geq \frac{2\log(\log(3))}{3} = a_3.$$

Hence, for $n \geq 3$ we have

$$\frac{n}{\phi(n)} \leq \frac{3\log(\log(n))}{2\log(\log(3))}.$$

The second inequality is well known, and, for instance, it can be deduce easily from the previous one for $n \geq 503$, and checked for small values of n. □

Lemma 2.3. *For every positive integer n, we have*

$$\frac{2^n n!}{n^{n-5}} \leq \frac{2^{18}18!}{18^{18-5}} < 80601.$$

Proof. One can check that the result hold true for $n \leq 18$. For $n \geq 18$, let $U_n = \frac{2^n n!}{n^{n-5}}$. Then

$$\begin{aligned}
\frac{U_{n+1}}{U_n} &= 2\left(\frac{n+1}{n}\right)^5 \left(\frac{n}{n+1}\right)^n \\
&\leq 2\left(\frac{19}{18}\right)^5 \left(\frac{n}{n+1}\right)^n \\
&\leq \left(\frac{19}{18}\right)^5 \left(\frac{18}{19}\right)^{18} \\
&< 1,
\end{aligned}$$

where we used the fact that $\left(\left(\frac{n}{n+1}\right)^n\right)_{n\geq 1}$ is a decreasing sequence. Hence the sequence $(U_n)_{n\geq 18}$ is decreasing, which proves the result. □

3 Proof of Theorem 1.2

We can now establish the proof of Theorem 1.2. Firstly, we will demonstrate a lower bound for $h(\alpha)$ depending on the multiplicative rank ρ of the conjugates of α, and on the degree d of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

Lemma 3.1. *Let $\alpha \in \overline{\mathbb{Q}}^*$ of degree d over $\mathbb{Q}$ and not a root of unity. Let ρ be the multiplicative rank of the conjugates of α. Define*

$$g_1(\rho, d) = \min_{1 \le r \le \rho} \left(d^{1/r} (1050 r^5 \log(3d))^{r(r+1)^2} \right)$$

and

$$g_2(\rho, d) = 10^{20} \rho^\rho \log\left(\log\left(6d^2\right)\right)^5.$$

Then:

$$h(\alpha) \ge \min\left(g_1(\rho, d), g_2(\rho, d)\right)^{-1}.$$

Proof. By Theorem 2.1 applied to $\mathbb{Q}(\alpha)$, and given that all conjugates of α over $\mathbb{Q}$ are in $\mathbb{Q}(\alpha)$ (since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois), we have, for every $1 \le r \le \rho$, that

$$h(\alpha) \ge d^{-1/r} (1050 r^5 \log(3d))^{-r(r+1)^2},$$

so $h(\alpha) \ge g_1(\rho, d)^{-1}$.

By Lemma 2.1, there exists $L \subset \mathbb{Q}(\alpha)$ and $k \ge 1$ such that $L/\mathbb{Q}$ is Galois, $[L : \mathbb{Q}] \le 135 \rho! 2^{\rho-1}$, $\mathbb{Q}(\zeta_k) \subset \mathbb{Q}(\alpha)$ and $\alpha^k \in L$. Set $M = \mathbb{Q}(\zeta_k)$. We have $M(\alpha) = \mathbb{Q}(\alpha) = L(\alpha)$. Notice that

$$[M(\alpha) : M] = [L(\alpha) : L] \frac{[L : \mathbb{Q}]}{[M : \mathbb{Q}]}.$$

Since α is a root of $X^k - \alpha^k \in L[X]$, we have $[L(\alpha) : L] \le k$. We also have $\phi(k) = [M : \mathbb{Q}]$. Therefore, we obtain

$$[M(\alpha) : M] \le k \frac{[L : \mathbb{Q}]}{[M : \mathbb{Q}]} \le \frac{k}{\phi(k)} [L : \mathbb{Q}].$$

By Lemma 2.2, we have

$$\frac{k}{\phi(k)} \le \frac{3 \log(\log(3k))}{2 \log(\log(3))},$$

so

$$[M(\alpha) : M] \le 405 \frac{\log(\log(3k))}{\log(\log(3))} \rho! 2^{\rho-2}.$$

We notice that $\phi(k) \le d$. By the last statement of Lemma 2.3, we have $\sqrt{k/2} \le \phi(k)$. Hence, we have $k \le 2d^2$, and so

$$[M(\alpha) : M] \le 405 \frac{\log\left(\log\left(6d^2\right)\right)}{\log(\log(3))} D \rho! 2^{\rho-2} \le 10^4 \rho! 2^\rho \log\left(\log\left(6d^2\right)\right).$$

By Lemma 2.3 we have

$$[M(\alpha) : M] \leq 10^9 \rho^{\rho-5} \log\left(\log\left(6d^2\right)\right).$$

By Theorem 2.2, applied to $\mathbb{Q}(\zeta_k)/\mathbb{Q}$, we have

$$h(\alpha) \geq [M(\alpha) : M]^{-1} \frac{\log\left(\log\left(5[M(\alpha) : M]\right)\right)^3}{\log(2[M(\alpha) : M])^4}.$$

Since the function

$$f(x) = \frac{1}{x} \frac{\log(\log(5x))^3}{\log(2x)^4}$$

is decreasing on the interval $[1, +\infty[$, setting

$$X(\rho, d) = 10^9 \rho^{\rho-5} \log\left(\log\left(6d^2\right)\right)$$

we deduce that

$$h(\alpha)^{-1} \leq X(\rho, d) \log(2X(\rho, d))^4 \leq 10^{20} \rho^{\rho} \log\left(\log\left(6d^2\right)\right)^5.$$

Hence $h(\alpha) \geq g_2(\rho, d)^{-1}$. This proves the lemma. □

Proof of Theorem 1.2. Now, we are ready to prove Theorem 1.2. Suppose, first, that $\rho \leq \log(3d)^{1/4}$. By Lemma 3.1, we get

$$\begin{aligned} h(\alpha)^{-1} &\leq g_2(\rho, d) = 10^{20} \left(\log(3d)^{1/4}\right)^{\log(3d)^{1/4}} \log\left(\log\left(6d^2\right)\right)^5 \\ &= \exp\left(20\log(10) + \log(3d)^{1/4} \log(\log(3d)^{1/4}) + 5\log(\log\left(\log\left(6d^2\right)\right))\right). \end{aligned}$$

So, we have

$$h(\alpha)^{-1} \leq \exp\left(20\log(10) + 6\log(3d)^{1/4} \log(\log(3d)))\right). \tag{1}$$

Now, we suppose that $\rho \geq \log(3d)^{1/4}$. We choose $r \in \mathbb{Z}$ such that $\log(3d)^{1/4} + 1 > r \geq \log(3d)^{1/4}$. In particular $r \leq \rho$. Then, thanks again to Lemma 3.1, we obtain

$$\begin{aligned} h(\alpha)^{-1} &\leq g_1(\rho, d) = d^{1/r} (1050 r^5 \log(3d))^{r(r+1)^2} \\ &\leq d^{1/\log(3d)^{1/4}} \left(1050(\log(3d)^{1/4} + 1)^5 \log(3d)\right)^{(\log(3d)^{1/4}+1)(\log(3d)^{1/4}+2)^2} \\ &\leq d^{1/\log(3d)^{1/4}} \left(2^{16} \log(3d)^{9/4}\right)^{2^3 \log(3d)^{3/4}} \\ &= \exp\left(\log(3d)^{3/4} + 2^3 \log(3d)^{3/4} \log(2^{16} \log(3d)^{9/4})\right). \end{aligned}$$

So, we have

$$h(\alpha)^{-1} \leq \exp\left(\log(3d)^{3/4} + 400\log(3d)^{3/4}\log(\log(3d))\right). \tag{2}$$

From (1) and (2), we obtain

$$h(\alpha)^{-1} \leq \exp\left(500\log(3d)^{3/4}\log(\log(3d))\right).$$

□

Acknowledgments

I am grateful to Gaël Rémond for comments and suggestions on an earlier draft of this article, and for pointing out the reference [Rém20].

References

[AD99] Francesco Amoroso and Sinnou David. The higher-dimensional Lehmer problem. *J. Reine Angew. Math.*, 513:145–179, 1999.

[AD00] Francesco Amoroso and Roberto Dvornicich. A lower bound for the height in abelian extensions. *J. Number Theory*, 80(2):260–272, 2000.

[AD07] Francesco Amoroso and Emmanuel Delsinne. An explicit relative lower bound for the height in an extension of an abelian extension. *Diophantine geometry*, 1–24, 2007.

[AM16] Francesco Amoroso and David Masser. Lower bounds for the height in Galois extensions. *Bull. Lond. Math. Soc.*, 48(6):1008–1012, 2016.

[AV12] Francesco Amoroso and Evelina Viada. Small points on rational subvarieties of tori. *Comment. Math. Helv.*, 87(2):355–383, 2012.

[AZ10] Francesco Amoroso and Umberto Zannier. A uniform relative Dobrowolski's lower bound over Abelian extensions. *Bull. Lond. Math. Soc.*, 42(3):489–498, 2010.

[BS96] Eric Bach and Jeffrey Shallit. Algorithmic number theory, Vol. 1: Efficient algorithms. *Cambridge, MA: The MIT Press*, 1996.

[Dob79] Edward Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34:391–401, 1979.

[Rém20] Gaël Rémond. Degré de définition des endomorphismes d'une variété abélienne. *J. Eur. Math. Soc. (JEMS)*, 22(9):3059–3099, 2020.

[Sch73] Andrzej Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24:385–399, 1973.

JONATHAN JENVRIN: Univ. Grenoble Alpes, CNRS, IF, 38000 Grenoble, France

E-mail adress : jonathan.jenvrin@univ-grenoble-alpes.fr