Lower bounds for the height in Galois extensions

F. Amoroso, D. Masser

Departement Mathematik und Informatik
Fachbereich Mathematik
Universität Basel
CH-4051 Basel

Preprint No. 2016-24
November 2016

www.math.unibas.ch
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 $\alpha$ 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 $\alpha$ and $\alpha_i$ are its algebraic conjugates. Recall that $h(\alpha) = 0$ if and only if $\alpha = 0$ or $\alpha$ 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 $\alpha$. Thus Breusch [5] proved it for non-reciprocal $\alpha$, 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 $\alpha \in \mathbb{Q}$ 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: June 29, 2016.*
where \( D = [K(\alpha_1, \ldots, \alpha_r) : K] \).

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 \( p \) be the multiplicative rank of the conjugates \( \alpha_1, \ldots, \alpha_d \) of \( \alpha \) over \( \mathbb{Q} \), and suppose \( \rho \geq 1 \). Then there exists a subfield \( L \subseteq F \) which is Galois over \( \mathbb{Q} \) of degree \( [L: \mathbb{Q}] = n \leq n(p) \) and an integer \( e \geq 1 \) such that \( \mathbb{Q}(\zeta_e) \subseteq F \) (for a primitive \( e \)th root of unity \( \zeta_e \)) 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 \( \beta_i = \alpha_i^e (i = 1, \ldots, d) \) and \( L = \mathbb{Q}(\beta_1, \ldots, \beta_d) \). The \( \mathbb{Z} \)-module
\[
\mathcal{M} = \{a_1 \beta_1^a \cdots \beta_d^a | a_1, \ldots, a_d \in \mathbb{Z}\}
\]
is torsion free (by the choice of \( e \)) and so, by the Classification Theorem for abelian groups, is free, of rank \( \rho \). This shows that the action of \( \text{Gal}(L/\mathbb{Q}) \) over \( \mathcal{M} \) defines an injective representation \( \text{Gal}(L/\mathbb{Q}) \to \text{GL}(\mathcal{M}) \). Thus \( \text{Gal}(L/\mathbb{Q}) \) identifies to a finite subgroup of \( \text{GL}(\mathcal{M}) \). But, by well-known results (see Remark 2.3 below), the cardinalities of the finite subgroups of \( \text{GL}(\mathcal{M}) \) are uniformly bounded by, say, \( n = n(p) \).

\[\square\]

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 Feit [8] (unpublished) shows that the orthogonal group \( O(p)(\mathbb{Z}) \) (of order \( 2^{p^2} \)) has maximal order for \( p = 1, 3, 5 \) and for \( p 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

We finally recall a well-known estimate on the Euler’s totient function \( \phi(\cdot) \) (see for instance [10, Theorem 328, p.267]):
\[
(2.1) \liminf_{n \to \infty} \frac{\phi(n) \log \log n}{n} = e^{-\gamma}.
\]

3. Main results

We now state two results about \( \alpha \) 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 \( \alpha \) over \( \mathbb{Q} \) which are multiplicatively independent (so that \( \alpha \) 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 $<_{\varepsilon}, \gg_{r,\varepsilon}$.

Let $\alpha_1, \ldots, \alpha_d$ (with $d \leq D$) be the conjugates of $\alpha$ 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 $[L : \mathbb{Q}] = n \leq n(r)$ and an integer $\varepsilon \geq 1$ such that $\mathbb{Q}(\zeta_n) \subseteq F$ and $\alpha^\varepsilon \in L$.

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

$$h(\alpha) = \frac{1}{e} h(\alpha^\varepsilon) \gg_{r,\varepsilon} \frac{1}{e}.  \tag{3.1}$$

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

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

(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

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

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 $\alpha$ of a Galois extension.

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

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

**Proof.** Let $r$ be the smallest integer $> 1/\varepsilon$. If $r \geq d$ then $d \leq 1 + 1/\varepsilon$ and $h(\alpha) \gg_{\varepsilon} 1$. So we can assume $r < d$. If $r$ among the conjugates of $\alpha$ 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 $\rho \geq 1$ of the conjugates of $\alpha$ is at most $r - 1 \leq 1/\varepsilon$. By Lemma 2.2 there exists a number field $L \subseteq \mathbb{Q}(\alpha)$ of degree $[L : \mathbb{Q}] = n \leq$
\[ n(\varepsilon) \text{ and an integer } e \geq 1 \text{ such that } \mathbb{Q}(\zeta_\varepsilon) \subseteq \mathbb{Q}(\alpha) \text{ and } \alpha^e \in L. \] As a consequence \( L(\alpha)/L \) is of degree \( e' \leq e \). The diagram

\[
\begin{array}{c}
\mathbb{Q}(\alpha) = L(\alpha) \\
\mathbb{Q}(\zeta_\varepsilon) \\
L \\
\mathbb{Q}(\zeta_\varepsilon) \\
k := L \cap \mathbb{Q}(\zeta_\varepsilon) \\
\mathbb{Q}
\end{array}
\]

shows that the degree of \( \alpha \) over \( \mathbb{Q}(\zeta_\varepsilon) \) is

\[
[\mathbb{Q}(\alpha) : L(\zeta_\varepsilon)] : [L(\zeta_\varepsilon) : \mathbb{Q}(\zeta_\varepsilon)] = e'[L(\zeta_\varepsilon) : \mathbb{Q}(\zeta_\varepsilon)]/[L(\zeta_\varepsilon) : L]
\]

which is

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

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

\[
h(\alpha) \gg_e d^{-2e}.
\]

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 \( \alpha = 1 + \zeta_\varepsilon \) with \( d = \phi(e) \) one has \( h(\alpha) \leq \log 2 \). Or \( \alpha = 2^{1/e} + \zeta_\varepsilon \), 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 \( h(\alpha) > 1 \) 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

   Available at http://www.birs.ca/workshops/2015/15w5054/report15w5054.pdf
<table>
<thead>
<tr>
<th>No.</th>
<th>Author</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-41</td>
<td>H. Harbrecht, W. L. Wendland, N. Zorii</td>
<td>Minimal energy problems for strongly singular Riesz kernels</td>
</tr>
<tr>
<td>2015-42</td>
<td>H. Harbrecht, M. Utzinger</td>
<td>On adaptive wavelet boundary element methods</td>
</tr>
<tr>
<td>2016-01</td>
<td>S. Iula, G. Mancini</td>
<td>Extremal functions for singular Moser-Trudinger embeddings</td>
</tr>
<tr>
<td>2016-02</td>
<td>J. K. Canci, L. Paladino</td>
<td>On preperiodic points of rational functions defined over $\mathbb{F}_p(t)$</td>
</tr>
<tr>
<td>2016-03</td>
<td>H. Harbrecht, R. Schneider</td>
<td>A note on multilevel based error estimation</td>
</tr>
<tr>
<td>2016-04</td>
<td>C. Urech</td>
<td>On homomorphisms between Cremona groups</td>
</tr>
<tr>
<td>2016-06</td>
<td>M. Dambrine, I. Greff, H. Harbrecht, B. Puig</td>
<td>Numerical solution of the homogeneous Neumann boundary value problem on domains with a thin layer of random thickness</td>
</tr>
<tr>
<td>2016-07</td>
<td>G. Alberti, G. Crippa, A. L. Mazzucato</td>
<td>Exponential self-similar mixing by incompressible flows</td>
</tr>
<tr>
<td>2016-08</td>
<td>M. Bainbridge, P. Habegger, M. Möller</td>
<td>Teichmüller curves in genus three and just likely intersections in $G^n_a \times G^n_a$</td>
</tr>
<tr>
<td>2016-09</td>
<td>Gabriel A. Dill</td>
<td>Effective approximation and Diophantine applications</td>
</tr>
<tr>
<td>2016-10</td>
<td>J. Blanc, S. Zimmermann</td>
<td>Topological simplicity of the Cremona groups</td>
</tr>
<tr>
<td>2016-11</td>
<td>I. Hedén, S. Zimmermann</td>
<td>The decomposition group of a line in the plane</td>
</tr>
<tr>
<td>2016-12</td>
<td>J. Ballani, D. Kressner, M. Peters</td>
<td>Multilevel tensor approximation of PDEs with random data</td>
</tr>
</tbody>
</table>

Preprints are available under https://math.unibas.ch/research/publications
LATEST PREPRINTS

No.  Author:  Title

2016-13  M. J. Grote, M. Kray, U. Nahum
Adaptive eigenspace method for inverse scattering problems in the frequency domain

2016-14  H. Harbrecht, M. Peters, M. Schmidlin
Uncertainty quantification for PDEs with anisotropic random diffusion

2016-15  F. Da Lio, L. Martinazzi
The nonlocal Liouville-type equation in $\mathbb{R}$ and conformal immersions of the disk with boundary singularities

2016-16  A. Hyder
Conformally Euclidean metrics on $\mathbb{R}^n$ with arbitrary total $Q$-curvature

2016-17  G. Mancini, L. Martinazzi
The Moser-Trudinger inequality and its extremals on a disk via energy estimates

2016-18  R. N. Gantner, M. D. Peters
Higher order quasi-Monte Carlo for Bayesian shape inversion

2016-19  C. Urech
Remarks on the degree growth of birational transformations

2016-20  S. Dahlke, H. Harbrecht, M. Utzinger, M. Weimar
Adaptive wavelet BEM for boundary integral equations: Theory and numerical experiments

2016-21  A. Hyder, S. Iula, L. Martinazzi
Large blow-up sets for the prescribed $Q$-curvature equation in the Euclidean space

2016-22  P. Habegger
The norm of Gaussian periods

2016-23  P. Habegger
Diophantine approximations on definable sets

2016-24  F. Amoroso, D. Masser
Lower bounds for the height in Galois extensions

Preprints are available under https://math.unibas.ch/research/publications