PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 6, June 2014, Pages 1893–1910
S 0002-9939(2014)11925-3
Article electronically published on March 3, 2014

ON FIELDS WITH PROPERTY (B)

FRANCESCO AMOROSO, SINNOU DAVID, AND UMBERTO ZANNIER

(Communicated by Matthew A. Papanikolas)

ABSTRACT. Let K be a number field and let L/K be an infinite Galois extension with Galois group G. Let us assume that $G/Z(G)$ has finite exponent. We show that L has the Property (B) of Bombieri and Zannier: the absolute and logarithmic Weil height on L^* is bounded from below outside the set of roots of unity by an absolute constant. We also discuss some features of Property (B): stability by algebraic extensions and relations with field arithmetic. As a side result, we prove that the Galois group over $\mathbb{Q}$ of the compositum of all totally real fields is torsion free.

1. INTRODUCTION

Let $h\colon \overline{\mathbb{Q}} \longrightarrow \mathbb{R}^+$ be the absolute and logarithmic Weil height. Assuming that $\alpha \in \overline{\mathbb{Q}}^*$ is not a root of unity, D. H. Lehmer ([20], §13, page 473) suggested that $[\mathbb{Q}(\alpha):\mathbb{Q}]h(\alpha)$ can be bounded below uniformly in α. Known as "Lehmer's problem" this question is still open, the best known result being a celebrated theorem of Dobrowolski ([12]) which proves it up to a positive ϵ. Nevertheless, significant progress has been made to understand the reach of this question. In particular, in the context of multiplicative groups, the Weil height is the normalized height, and in the higher dimensional case, one can formulate a natural generalization of Lehmer's problem in the following way (see [1] and [25] for details and context).

For simplicity we fix the natural compactification $\mathbb{G}_{\mathrm{m}}^n \hookrightarrow \mathbb{P}^n$ of $\mathbb{G}_{\mathrm{m}}^n$ and denote by h the Weil height on $\mathbb{P}^n(\overline{\mathbb{Q}})$. One says that an algebraic set B of $\mathbb{G}_{\mathrm{m}}^n$ is *torsion* if its geometric components are translates of subtori by torsion points.

Let $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\overline{\mathbb{Q}})$ and denote by $B(\boldsymbol{\alpha}) \subseteq \mathbb{G}_{\mathrm{m}}^n$ the smallest (for the inclusion) torsion subvariety defined over $\mathbb{Q}$ and containing $\boldsymbol{\alpha}$. We define

$$\omega(\boldsymbol{\alpha}) = \inf_Z \left(\frac{\deg(Z)}{\deg(B(\boldsymbol{\alpha}))} \right)^{1/\mathrm{codim}_{B(\boldsymbol{\alpha})}(Z)},$$

where Z runs over subvarieties $Z \subsetneq B(\boldsymbol{\alpha})$ defined over $\mathbb{Q}$ and containing $\boldsymbol{\alpha}$.

With this notation, one can conjecture (for $n = 1$, the statement is precisely Lehmer's problem):

Conjecture 1.1. *There exists a positive real number $c(n) > 0$ such that for every* non-torsion $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n(\overline{\mathbb{Q}})$,

$$h(\alpha) \geq \frac{c(n)}{\omega(\boldsymbol{\alpha})}.$$

Received by the editors January 18, 2012 and, in revised form, July 4, 2012.
2010 *Mathematics Subject Classification.* Primary 11G50; Secondary 12E30.
The first and second authors were partially supported by ANR "HaMoT".
The third author was partially supported by ERC "Diophantine Problems".

In a less geometric tone, following the works of the first author with Dvornicich and the third author ([2], [4]), one can conjecture a *relative version* of Lehmer's problem, where the ground field $\mathbb{Q}$ is replaced by its maximal abelian extension:

Conjecture 1.2. *There exists a positive real number $c > 0$ such that for every* non-torsion $\alpha \in \mathbb{G}_{\mathrm{m}}(\overline{\mathbb{Q}})$,

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}]} \ .$$

As for the classical Lehmer's problem, this conjecture is proved up to a positive ϵ (see [4]). Interestingly, it is easy to remark (see [21], Proposition 2.5, for a more general statement) that the two dimensional case of Conjecture 1.1 implies the relative Lehmer problem (Conjecture 1.2), and this can be explained by the fact that $\mathbb{Q}^{\mathrm{ab}}$ is the field $\mathbb{Q}((\mathbb{G}_{\mathrm{m}})_{\mathrm{tors}})$ generated by all the torsion points of $\mathbb{G}_{\mathrm{m}}$ (when working with abelian varieties, one should replace $\mathbb{Q}^{\mathrm{ab}}$ by the field generated by the torsion over some field of definition).

However, recent works suggest that this geometric interpretation is not sufficient to fully put Lehmer's problem in its most natural and general context (for instance, see [25]). The purpose of this work is to proceed towards a better understanding of which ground fields can be good candidates to formulate Lehmer's problem.

With this point of view, two natural concepts arise. For a field K to qualify as a good candidate to replace $\mathbb{Q}$ in Lehmer's problem, the Weil height should *at least* be bounded below outside the roots of unity. Indeed, Conjecture 1.2 implies that $\mathbb{Q}^{\mathrm{ab}}$ satisfies this property. Secondly, for diophantine geometry to be efficient, one needs finiteness properties for the height. We thus introduce these notions. Following Bombieri and the third author [9], we set:

Definition 1.3. Let $\mathcal{A}$ be a subset of the set of algebraic numbers.

(i) We say that $\mathcal{A}$ has the *Bogomolov Property* (B) if there exists a real number $T_0 = T_0(\mathcal{A}) > 0$ such that the set of non-zero $\alpha \in \mathcal{A}$ of height $< T_0$ consists of all roots of unity in $\mathcal{A}$.

(ii) We say that $\mathcal{A}$ has the *Northcott Property* (N) if for any positive real number T the set of $\alpha \in \mathcal{A}$ of height $< T$ is finite.

Of course, every number field has Properties (B) and (N). Thus it should be noted that for these questions to be non-trivial, the algebraic fields considered need to be *infinite* extensions of $\mathbb{Q}$.

In this paper, we shall explore these properties and suggest some questions, mainly concentrating on Property (B). A positive answer would permit to some extent a unification of the scattered examples of fields which are known to satisfy (B) or (N).

There are several interesting examples of subfields of $\overline{\mathbb{Q}}$ with Property (B).

(i) A first class of fields with Property (B) is provided by fields with bounded local degrees at some finite place. Let K be a number field and L/K be an infinite extension. Fix a non-archimedean valuation v of K. We say that L/K has bounded local degree at v if there exists an integer d_0 such that for every extension w of v to L we have $[L_w : K_v] \leq d_0$. By a result of Bombieri and the third author (see [9], Theorem 2), a Galois extension $L/\mathbb{Q}$ with bounded local degree at some rational prime satisfies Property (B). One can also put in this class the field $\mathbb{Q}^{\mathrm{tr}}$ of all totally real algebraic numbers (the natural archimedean analogue would be to say that L

has a *bounded degree at* ∞ if it is totally real). Property (B) has been established for $\mathbb{Q}^{\mathrm{tr}}$ by Schinzel; see [27] (also see the work of Smyth [28]).

(ii) Secondly, the maximal abelian $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ satisfies (B) (see [2]), thus solving the case $[\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}] = 1$ of Conjecture 1.2. More generally, the abelian closure K^{ab} of a number field K satisfies (B) (see [4]). Moreover, Property (B) holds uniformly in $[K : \mathbb{Q}]$; the height on $(K^{\mathrm{ab}})^*$ outside roots of unity is bounded from below by a positive constant depending only on $[K : \mathbb{Q}]$ (see [5]).

(iii) A third class has recently been exhibited by Habegger [16]. Let E be an elliptic curve defined over $\mathbb{Q}$. Then the field $\mathbb{Q}(E_{\mathrm{tors}})$ obtained by adjoining all torsion points of E has the Bogomolov Property. However, if E does not have complex multiplication, then there are no number fields K such that $\mathbb{Q}(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$ (see [16]).

Many other scattered examples can be exhibited. For instance, it can be noted that if $L/\mathbb{Q}$ is an extension such that any number field contained in L has a large enough discriminant, then Property (B) can be derived.

However the examples (ii) and (iii) are motivated by group theoretic properties. This is clear for example (ii). For the the case of $\mathbb{Q}(E_{\mathrm{tors}})$, the Frobenius at finite super singular primes lies in the center of the Galois group. Also, when we have ramification, Lubin-Tate theory provides a suitable replacement of the Frobenius inside a higher ramification group having a sufficiently large centralizer (see [16] for details). Example (i) can also be better understood by group theoretic properties, by considering Galois extensions having uniformly bounded local degrees at *every* finite place. Indeed, this is equivalent to asking that the corresponding Galois group have a finite exponent, as is proven by S. Checcoli (see [10] for a more precise statement).

Our first aim is to suggest a unification of the first two classes which seem more closely related to $\mathbb{G}_{\mathrm{m}}$. In heuristic terms, one would like to find a Property (Π) such that if G is a Galois group for which (Π) is true, then any Galois extension $L/\mathbb{Q}$ with Galois group G has the Bogomolov Property. Such a statement would be even better if one could ensure that assuming G *does not* satisfy (Π), then there is at least one normal extension $L/\mathbb{Q}$ with group G that does not have the Bogomolov Property. Though we are far from such an understanding of the situation, we would like to suggest the following problem along these lines:

Problem 1.4. Let $K/\mathbb{Q}$ be an extension with bounded local degree at some rational prime. Is it true that K^{ab} has Property (B)?

The first result of this article is a partial answer to this problem. In section 4 we prove the following theorem, which is enough to contain both the first two classes of examples quoted above and is thus a generalization of both [9], Theorem 2, and [5], Theorem 1.2:

Theorem 1.5. *Let K be a number field and let L/K be an infinite Galois extension with Galois group G. Let $E \subseteq L$ be the subfield fixed by $Z(G)$ and assume that E/K has local degree at some non-archimedean valuation v of K bounded by d_0. Then L has Property (B) uniformly in v, d_0 and $[K : \mathbb{Q}]$.*

More explicitly, there exists a positive function c which depends effectively only on v, d_0 and $[K : \mathbb{Q}]$ such that for any $\alpha \in L^*$ which is not a root of unity we have $h(\alpha) \geq c$.

As one can see, in this result, the main point is that L *need not* be abelian over the base field K, nor does it *need* to be of bounded local degree.

If one wants to state results and questions purely in group theoretic terms as in the heuristics above, it is easy to slightly weaken either Problem 1.4 or Theorem 1.5 by considering Galois extensions having uniformly bounded local degrees at *every* finite place. Indeed, as already remarked, this is equivalent to asking that the corresponding Galois group have a finite exponent ([10]). To make things explicit, here is how the weak form of Problem 1.4 would read:

Problem 1.6. Let N be an abelian group and H be a group of finite exponent. Assume that the group G is an extension of H by N, i.e. fits in an exact sequence:

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1 \ .$$

Then is it true that if K is a number field and L/K is a normal extension with Galois group G that L satisfies (B)?

Similarly, our Theorem 1.5 implies:

Corollary 1.7. *Let K be a number field and let L/K be an infinite Galois extension with Galois group G. Let us assume that $G/Z(G)$ has finite exponent b. Then L has Property (B) uniformly in b and $[K : \mathbb{Q}]$.*

We now move to the question of the stability of these properties under finite extension. Assume that L/K is an abelian extension of a number field K. By the main theorem of [4], F has Property (B). Similarly, if $L/\mathbb{Q}$ has bounded local degree at some rational prime, then $F/\mathbb{Q}$ has the same property and thus, by [9], it has Property (B). Therefore the following question arises naturally.

Problem 1.8. Let L be a field with Property (B) and let F/L be a finite extension. Is it true that F necessarily has Property (B)?

In section 5 we give a *negative* answer to this question and we provide some related remarks about possible ways of strengthening the requirements to ensure stability. On the other hand, if an extension $L/\mathbb{Q}$ has Property (N), then every finite extension F/L again has (N) (cf. Theorem 2.1 of [13]). Thus Property (B) and Property (N) behave in radically different ways under finite extension.

One key example to keep in mind while studying the behavior of (B) under extension is the compositum $\mathbb{Q}^{\mathrm{tr}}$ of all totally real fields. We devote section 7 to its study and prove that the Galois group of $\mathbb{Q}^{\mathrm{tr}}$ over $\mathbb{Q}$ is torsion free (Theorem 5.4). We need this result of independent interest in section 5, and it was apparently not known.

Our section 6 is more speculative. We explore possible relations between Property (B) and field arithmetic. Two central definitions in this area are Pseudo Algebraically Closed and Hilbertian fields. We recall that a field K is Pseudo Algebraically Closed (PAC) if each absolutely irreducible variety defined over K has a K-rational point (see [15], chapter 11, for more details). A field K is Hilbertian if it satisfies Hilbert's Irreduciblity Theorem: for every irreducible $f \in K[x, y]$ which is separable in x there exists $a \in K$ such that $f(x, a)$ is irreducible over K (see [15], chapter 12, for more details). We consider the following problems. Does there exist a PAC field $K \subseteq \overline{\mathbb{Q}}$ which satisfies (B)? What are the relations between (B) and Hilbertianity? We give some evidence for a negative answer to the first question and we provide examples of a Hilbertian (respectively non-Hilbertian) field which does not satisfy (respectively which satisfies) Property (B).

2. Notation and auxiliary results

Let K be a number field. Given a place v of K we denote by $|\cdot|_v$ the corresponding absolute value normalized to induce the underlying standard absolute value on $\mathbb{Q}$.

We shall use the following two lemmas. The first one is a technical observation that enables a form of "acceleration of convergence". It helps us to simplify some later computations and to avoid having to work with a large enough rational prime (which would weaken lower bounds). It is also of independent interest.

Lemma 2.1. *Let K be a number field, v be a finite place of K over a rational prime p and $\rho > 0$. Let γ_1, $\gamma_2 \in \mathcal{O}_K$ be such that $|\gamma_1 - \gamma_2|_v \leq p^{-\rho}$. Then for any non-negative integer λ we have $|\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda}|_v \leq p^{-s_{p,\rho}(\lambda)}$ with $s_{p,\rho}(\lambda) \to +\infty$ for $\lambda \to +\infty$.*

More precisely, let us define an integer $k = k_{p,\rho}$ by $k = 0$ if $(p-1)\rho > 1$ and by

$$p^{k-1}(p-1)\rho \leq 1 < p^k(p-1)\rho$$

otherwise. Then we can take

$$s_{p,\rho}(\lambda) = p^k\rho + \max(0, \lambda - k) \ .$$

Proof. Let ζ_{p^λ} be a primitive root of order p^λ. Let us moreover denote by the same letter v the only valuation of $K(\zeta_{p^\lambda})$ extending v. We write

$$\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda} = (\gamma_1 - \gamma_2) \prod_{j=1}^{\lambda} \prod_{\zeta_{p^j}} (\gamma_1 - \zeta_{p^j}\gamma_2),$$

where the inner product is taken on the roots of unity ζ_{p^j} of order p^j. The ultrametric inequality and the fact that p is totally ramified in $\mathbb{Q}(\zeta_{p^j})$ shows that

$$\begin{aligned} |\gamma_1 - \zeta_{p^j}\gamma_2|_v &= |\gamma_1 - \gamma_2 + (1 - \zeta_{p^j})\gamma_2|_v \\ &\leq \max(p^{-\rho}, p^{-1/p^{j-1}(p-1)}) \\ &= p^{-\min(p^{j-1}(p-1)\rho, 1)/p^{j-1}(p-1)} \ . \end{aligned}$$

Then $|\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda}|_v \leq p^{-s}$ with

$$\begin{aligned} s &= \rho + \sum_{j=1}^{\lambda} \min(p^{j-1}(p-1)\rho, 1) \\ &= \rho + \sum_{j=1}^{k} p^{j-1}(p-1)\rho + \sum_{j=k+1}^{\lambda} 1 = p^k\rho + \max(0, \lambda - k). \end{aligned}$$

□

Next comes a second technical estimate. Assuming a suitable metric property, we check that the predictable lower bound for the height follows. This is basically straightforward, but we feel that a self-contained statement enables one to separate the height machine from the metric inputs. It can also serve as a useful future reference. Note that this argument has already been used implicitly in the proofs of [2], Proposition 1, and of [5], Proposition 3.2.

Lemma 2.2. *Let L/K be a Galois extension of number fields and let $\sigma \in \mathrm{Gal}(L/K)$. Let $\wp$ be a prime of $\mathcal{O}_K$ over the rational prime p. Also let a, $b \geq 1$ be rational integers and $\rho > 0$. Let us assume that*

$$\forall \gamma \in \mathcal{O}_L, \quad \forall v \mid \wp, \qquad |\gamma^a - \sigma(\gamma)^b|_v \leq p^{-\rho} \ .$$

Then for every $\alpha \in L$ such that $\alpha^a \neq \sigma(\alpha)^b$ we have

$$h(\alpha) \geq \frac{1}{a+b}\left(\frac{[K_\wp : \mathbb{Q}_p]}{[K:\mathbb{Q}]}\rho \log p - \log 2\right) \ .$$

Proof. Let v be a place of L, normalized to induce the underlying standard place on $\mathbb{Q}$. We shall estimate $|\alpha^a - \sigma(\alpha)^b|_v$. Suppose that we start with $v \mid \wp$.

By the Strong Approximation Theorem, there exists an integer $\beta \in \mathcal{O}_L$ such that $\alpha\beta$ is an integer and

$$|\beta|_v = \max\{1, |\alpha|_v\}^{-1}$$

(see [2], Lemma 1, for details). Then we have $|(\alpha\beta)^a - \sigma(\alpha\beta)^b|_v \leq p^{-\rho}$ and $|\beta^a - \sigma(\beta)^b|_v \leq p^{-\rho}$. Using the ultrametric inequality, we deduce that

$$\begin{aligned} |\alpha^a - \sigma(\alpha)^b|_v &= |\beta|_v^{-a}|(\alpha\beta)^a - \sigma(\alpha\beta)^b + (\sigma(\beta)^b - \beta^a)\sigma(\alpha)^b|_v \\ &\leq c(v)\max(1,|\alpha|_v)^a \max(1,|\sigma(\alpha)|_v)^b \end{aligned}$$

with $c(v) = p^{-\rho}$. This last inequality plainly holds for an arbitrary place w of L with

$$c(w) = \begin{cases} 1, & \text{if } w \nmid \infty,\ w \nmid \wp\ , \\ 2, & \text{if } w \mid \infty\ . \end{cases}$$

Applying the product formula to $\alpha^a - \sigma(\alpha)^b$ we get

$$\begin{aligned} 0 &= \sum_w \frac{[L_w:\mathbb{Q}_w]}{[L:\mathbb{Q}]} \log |\alpha^a - \sigma(\alpha)^b|_w \\ &\leq \sum_w \frac{[L_w:\mathbb{Q}_w]}{[L:\mathbb{Q}]} \left(\log c(w) + a\log\max\{1,|\alpha|_w\} + b\log\max\{1,|\sigma(\alpha)|_w\}\right) \\ &= \left(\sum_{w\mid\infty} \frac{[L_w:\mathbb{Q}_w]}{[L:\mathbb{Q}]}\right)\log 2 - \left(\sum_{w\mid\wp} \frac{[L_w:\mathbb{Q}_w]}{[L:\mathbb{Q}]}\right)\rho\log p + ah(\alpha) + bh(\sigma(\alpha)) \\ &= \log 2 - \frac{[K_\wp:\mathbb{Q}_p]}{[K:\mathbb{Q}]}\rho\log p + (a+b)h(\alpha)\ . \end{aligned}$$

The conclusion follows. □

We now fix some notation which we use in the next two sections.

Let K be a number field of degree d over $\mathbb{Q}$. We consider a finite Galois extension L/K of Galois group G. Let N be a normal subgroup of G contained in $Z(G)$. We let $E = L^N$ be the fixed field of N. We remark that N is abelian (since it is contained in $Z(G)$). Thus L/E is an abelian extension of Galois group N.

We fix a prime ideal $\mathfrak{q}$ of $\mathcal{O}_E$. Let $\wp = \mathfrak{q} \cap \mathcal{O}_K$ and let $(p) = \wp \cap \mathbb{Z}$. We define d_0 as the local degree $[E_\mathfrak{q} : K_\wp]$.

We also denote by $\boldsymbol{\mu} \subset \mathbb{Q}^{\mathrm{ab}}$ the group of roots of unity and by $\boldsymbol{\mu}_{p^\infty} \subset \boldsymbol{\mu}$ the subgroup of roots of unity of order a power of p.

3. A conditional result

The main result of this section is the following generalization of Proposition 3.2 of [5]. This is where we input the metric property into which we shall feed Lemma 2.2. Assume first that $\mathfrak{q}$ does not ramify in $\mathcal{O}_L$. The point is to note that with a bounded local degree downstairs, the Frobenius morphisms of the primes of L

over $\mathfrak{q}$ can to some extent be glued together above. A similar consideration holds when $\mathfrak{q}$ ramifies in $\mathcal{O}_L$.

Proposition 3.1. *Let $\alpha \in L^* \backslash \boldsymbol{\mu}$. Assume further that for any non-trivial $\tau \in \mathrm{Gal}(L/E)$,*

$$\tau(\alpha)/\alpha \notin \boldsymbol{\mu}_{p^\infty} \ . \tag{3.1}$$

Then

$$h(\alpha) \geq c$$

for some $c > 0$ depending only on p, d_0 and d.

Furthermore, one can relax the assumption (3.1) *by requiring instead that for every $\tau \in \mathrm{Gal}(L/E)$,*

$$\tau(\alpha)/\alpha \notin \boldsymbol{\mu}_{p^\infty} \backslash \{1\} \ . \tag{3.2}$$

Proof. Note first that the supplement is trivial. Indeed $\mathrm{Gal}(E(\alpha)/E)$ is a normal subgroup of $\mathrm{Gal}(E(\alpha)/K)$ contained in the center, so replacing L by $E(\alpha)$ if necessary, we can assume $L = E(\alpha)$, and in this case (3.2) reduces to (3.1).

A first case occurs when $\mathfrak{q}$ does not ramify in L. Let ϕ be the Frobenius automorphism of $\mathfrak{Q}/\mathfrak{q}$, where $\mathfrak{Q}$ is any prime of $\mathcal{O}_L$ over $\mathfrak{q}$. Since L/E is abelian, ϕ does not depend on the choice of $\mathfrak{Q}$. Thus for any $\gamma \in \mathcal{O}_L$,

$$\gamma^q \equiv \phi(\gamma) \bmod \mathfrak{q}\mathcal{O}_L \ ,$$

where q is the norm of $\mathfrak{q}$. Now let $\mathfrak{q}'$ be another prime ideal of $\mathcal{O}_E$ over $\wp$, fix a prime $\mathfrak{Q}'$ of $\mathcal{O}_L$ over $\mathfrak{q}'$ and let ϕ' be the Frobenius of $\mathfrak{Q}'/\mathfrak{q}'$. Then ϕ and ϕ' are both in N and are conjugate in G. Since N is contained in $Z(G)$ we deduce that $\phi' = \phi$. This shows that for any $\gamma \in \mathcal{O}_L$ and for any place v of L with $v \,|\, \wp$ we have

$$|\gamma^q - \phi(\gamma)|_v \leq p^{-1/e_0} \ ,$$

where e_0 is the ramification index of $\mathfrak{q}$ over $\wp$.

Since α is not a root of unity, $\alpha^q - \phi(\alpha) \neq 0$. Thus, we can apply Lemma 2.2 and obtain

$$h(\alpha) \geq \frac{1}{q+1} \left(\frac{[K_\wp : \mathbb{Q}_p]}{de_0} \log p - \log 2 \right) \ .$$

This lower bound is non-trivial only if $p^{[K_\wp : \mathbb{Q}_p]} \geq 2^{de_0}$. In order to avoid this restriction on the prime p, we first use the acceleration lemma, Lemma 2.1.

This lemma shows that there exists λ depending only on p, on e_0 and on d such that

$$|\gamma^{qp^\lambda} - \phi(\gamma)^{p^\lambda}|_v \leq p^{-2d} \ .$$

Since α is not a root of unity, $\alpha^{qp^\lambda} - \phi(\alpha)^{p^\lambda} \neq 0$. By Lemma 2.2

$$h(\alpha) \geq \frac{1}{p^\lambda(q+1)} (2[K_\wp : \mathbb{Q}_p] \log p - \log 2) \geq \frac{\log 2}{p^\lambda(q+1)} = c_1,$$

where $c_1 > 0$ clearly depends only on p, d_0 and d since $q \leq p^{d_0}$ and $e_0 \leq d_0$.

Assume now that $\wp$ is ramified in L and let, as in [5], Proposition 2.3,

$$H_\mathfrak{q} := \{\tau \in N \text{ such that } \forall \gamma \in \mathcal{O}_L, \ \tau\gamma^q \equiv \gamma^q \bmod \mathfrak{q}\mathcal{O}_L\},$$

where q is the norm of $\mathfrak{q}$. By the quoted proposition, $H_\mathfrak{q}$ is non-trivial. As in the non-ramified case, let $\mathfrak{q}'$ be another prime ideal of $\mathcal{O}_E$ over $\wp$. Then $H_\mathfrak{q}$ and $H_{\mathfrak{q}'}$ are both subgroups of N and are conjugate in G. Since N is contained in $Z(G)$

we deduce that $H_{\mathfrak{q}'} = H_{\mathfrak{q}}$. Let τ be a non-trivial automorphism of this subgroup. Then, for any $\gamma \in \mathcal{O}_L$ and for any place v of L with $v \mid \wp$ we have

$$|\gamma^q - \tau(\gamma)^q|_v \leq p^{-1/e_0} \ ,$$

where e_0 is the ramification index of $\mathfrak{q}$ over $\wp$. We use Lemma 2.1 and Lemma 2.2 as in the first part of the proof. We remark that $\alpha^{qp^\lambda} - \tau(\alpha)^{qp^\lambda} \neq 0$ thanks to (3.1). We get $h(\alpha) \geq c_2$ for some $c_2 > 0$ depending only on p, d_0 and d. It is now enough to choose $c = \min(c_1, c_2)$. □

4. An unconditional result and the proof of Theorem 1.5

The radical reduction of [5], section 4, does not apply in the present situation. Indeed, following the beginning of the proof of Proposition 4.3 in [5], k is not necessarily a power of a prime and so we cannot bound the degree of $E(\zeta_k)/E$ in terms of d_0 and d. Nevertheless, we can modify the argument of [5] in such a way that it applies in the present situation. As an extra bonus the proof becomes simpler. Indeed, in [5] we perform an unnecessary reduction, using in two different steps essentially the same argument. This new approach could also be of independent interest and applicable to a close situation, namely to the relative lower bound ([4]) and to the subsequent generalizations of both abelian and relative lower bounds (see [8], [11], [24], [16]), where a kind of descent step is always used.

We first state a simplified and slightly precise version of a special case of [5], Lemma 4.2. The present statement applies only to subgroups of $(\mathbb{Z}/k\mathbb{Z})^*$ for k a prime power, but this is enough for our purposes.

Lemma 4.1. *Let p be a rational prime, k be a power of p and B be a positive integer. Then, for every subgroup H of $(\mathbb{Z}/k\mathbb{Z})^*$ of index $< B$, there are integers x, y such that $x \bmod k \in H$, $y \bmod k \in H$ and*

$$2 < y - x < 6B \ .$$

Proof. The proof is a straightforward application of the box principle. We give some details for the sake of completeness. Let $\Lambda = \{x \in \mathbb{N} \mid x \bmod k \in H\}$ and define, for $j \in \mathbb{N}$, the real interval

$$I_j = [6(j-1)B, 6jB) \ .$$

Assume by contradiction

$$\forall j \in \mathbb{N}, \qquad |I_j \cap \Lambda| \leq 3 \ .$$

Let J be a large enough integer and put $r = [6JB/k]$. Then

$$r|H| = |\Lambda \cap [0, rk)| \leq |\Lambda \cap [0, 6JB)| \leq 3J,$$

which implies $2B|H| \leq 6JB/r \leq k(r+1)/r$. Letting $J \to +\infty$ we get a contradiction:

$$2B|H| \leq k \leq 2(1-1/p)k = 2|(\mathbb{Z}/k\mathbb{Z})^*| < 2B|H| \ .$$

Thus there exist integers $x = x_1 < x_2 < x_3 < x_4 = y$ in one $I_j \cap \Lambda$, that is, such that $x_i \bmod k \in H$ and $y - x < 6B$. □

We can now prove an unconditional version of Proposition 3.1. Note that the main argument of the proof has a cohomological flavor.

Proposition 4.2. *Let $\alpha \in L^* \backslash \boldsymbol{\mu}$. Then*

$$h(\alpha) \geq c'$$

for some $c' > 0$ depending only on p, d_0 and d.

Proof. There exist $k = p^l$ ($l \geq 0$) and a primitive k-root of unity $\zeta_k \in L$ such that

$$L \cap \mathbb{Q}(\boldsymbol{\mu}_{p^\infty}) = L \cap \mathbb{Q}(\zeta_k) \ .$$

We identify $\mathrm{Gal}(E(\zeta_k)/E)$ to a subgroup of $(\mathbb{Z}/k\mathbb{Z})^*$ of index, say $B-1$. By Galois theory, $B - 1 = [E \cap \mathbb{Q}(\zeta_k) : \mathbb{Q}]$. Since k is a power of p, the prime p is totally ramified in $E \cap \mathbb{Q}(\zeta_k)$. This shows that $B - 1 \leq e(\mathfrak{q}|p) \leq d_0 d$. By Lemma 4.1 there exist σ_1, $\sigma_2 \in \mathrm{Gal}(E(\zeta_k)/E)$ such that $\sigma_i \zeta_k = \zeta_k^{g_i}$ with $g = g_2 - g_1$ satisfying

$$2 < g < 6(d_0 d + 1) \ . \tag{4.1}$$

Let $\tilde{\sigma}_i \in \mathrm{Gal}(L/E)$ extending σ_i. We want to apply Proposition 3.1 with $\alpha \leftarrow \beta$, where

$$\beta = \frac{\tilde{\sigma}_2(\alpha)}{\alpha^g \tilde{\sigma}_1(\alpha)} \ . \tag{4.2}$$

To do this we need to prove that $\beta \notin \boldsymbol{\mu}$ and that $\tau(\beta)/\beta \notin \boldsymbol{\mu}_{p^\infty} \backslash \{1\}$ for any $\tau \in \mathrm{Gal}(L/E)$. Let us verify these requirements. We argue by contradiction.

Let us first assume that $\beta \in \boldsymbol{\mu}$. Then, by (4.2),

$$gh(\alpha) = h(\alpha^g) = h(\tilde{\sigma}_2(\alpha)/\tilde{\sigma}_1(\alpha)) \leq 2h(\alpha) \ .$$

Since $g > 2$ by (4.1) we get $\alpha \in \boldsymbol{\mu}$. Contradiction.

Let us now assume that there exists $\tau \in \mathrm{Gal}(L/E)$ such that $\theta := \tau(\beta)/\beta \in \boldsymbol{\mu}_{p^\infty} \backslash \{1\}$. Let $\eta = \tau(\alpha)/\alpha$. Apply (4.2) and its conjugate by τ, taking into account that we are working in an abelian extension of E. We obtain

$$\theta = \frac{\tau(\beta)}{\beta} = \frac{\tau\tilde{\sigma}_2(\alpha)}{\tau(\alpha^g)\tau\tilde{\sigma}_1(\alpha)} \left(\frac{\tilde{\sigma}_2(\alpha)}{\alpha^g \tilde{\sigma}_1(\alpha)} \right)^{-1} = \frac{\tilde{\sigma}_2(\eta)}{\eta^g \tilde{\sigma}_1(\eta)} \ .$$

Hence

$$gh(\eta) \leq 2h(\eta) \ ,$$

which implies $h(\eta) = 0$ by (4.1). Thus $\eta \in \boldsymbol{\mu}$. Write η as $\eta = \eta_1 \eta_2$ with $\eta_1 \in \boldsymbol{\mu}_{p^\infty}$ and with η_2 of order not divisible by p. By Bezout's identity, $\eta_1 \in \mathbb{Q}(\eta) \subseteq L$. Thus there exists an integer a such that $\eta_1 = \zeta_k^a$. By the choice of $\tilde{\sigma}_i$ we see that

$$\frac{\tilde{\sigma}_2(\eta_1)}{\eta_1^g \tilde{\sigma}_1(\eta_1)} = 1 \ .$$

Thus

$$\theta = \frac{\tilde{\sigma}_2(\eta_2)}{\eta_2^g \tilde{\sigma}_1(\eta_2)}$$

has order not divisible by p. But $\theta \in \boldsymbol{\mu}_{p^\infty}$ and $\theta \neq 1$. Contradiction.

Applying (3.1) with $\alpha \leftarrow \beta$ we get $h(\beta) \geq c$. By (4.1) and (4.2),

$$h(\beta) \leq (g+2)h(\alpha) \leq (6d_0 d + 7)h(\alpha) \ .$$

Thus

$$h(\alpha) \geq c'$$

with $c' = c/(6d_0 d + 7)$. □

We are now in a position to prove Theorem 1.5. Let K be a number field and let L/K be an infinite Galois extension with Galois group G. Let $E \subseteq L$ be the subfield fixed by $Z(G)$ and assume that E/K has local degree at some prime $\wp$ bounded by d_0. Let $\alpha \in L^*$ not be a root of unity. We choose a subfield $L' \subseteq L$ containing α and such that L'/K is a finite Galois extension. We put $E' = L' \cap E$. Then it is easy to see that L'/E' is Galois and $\mathrm{Gal}(L'/E')$ is contained in the center of $\mathrm{Gal}(L'/K)$. Moreover, E'/K has local degree at $\wp$ bounded by d_0. By Proposition 4.2, the height of α is bounded from below by a positive constant depending only on $\wp$, d_0 and $[K : \mathbb{Q}]$. Theorem 1.5 follows.

5. Property (B) and field extensions

In this section we show that Property (B) is not generally preserved under finite extension. As remarked in the introduction, this on the contrary holds for Property (N).

Let $\mathbb{Q}^{\mathrm{tr}}$ be the compositum of all totally real extensions. Thus $\mathbb{Q}^{\mathrm{tr}}$ is a Galois extension of $\mathbb{Q}$ and $\alpha \in \mathbb{Q}^{\mathrm{tr}}$ if and only if α is totally real. We denote by i a square root of -1 in $\overline{\mathbb{Q}}$. Note that $\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}$ is also Galois, as the composite of the Galois extensions $\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q}$ and $\mathbb{Q}(i)/\mathbb{Q}$. Let τ be the generator of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}^{\mathrm{tr}})$. Then for any $\mathbb{Q}$-embedding $\sigma\colon \mathbb{Q}^{\mathrm{tr}}(i) \hookrightarrow \mathbb{C}$ we have $\overline{\sigma} = \sigma\tau$. This implies that if an archimedean absolute value of $\alpha \in \mathbb{Q}^{\mathrm{tr}}(i)$ is 1, then all its archimedean absolute values are equal to 1. The following lemma shows that the converse is also true.

Lemma 5.1. *Let $\alpha \in \overline{\mathbb{Q}}$ be such that all its archimedean absolute values are equal to 1. Then $\alpha \in \mathbb{Q}^{\mathrm{tr}}(i)$.*

Proof. We define

$$a = \frac{1}{2}(\alpha - \alpha^{-1}), \quad b = \frac{1}{2i}(\alpha - \alpha^{-1}) \ .$$

Then $\alpha = a + bi$ and $a, b \in \mathbb{Q}^{\mathrm{tr}}$. Indeed, let $\sigma\colon \mathbb{Q}^{\mathrm{tr}}(i) \hookrightarrow \mathbb{C}$. Since $1 = |\sigma\alpha|^2 = \sigma\alpha \cdot \overline{\sigma\alpha}$ we have

$$\sigma a = \frac{1}{2}(\sigma\alpha + \overline{\sigma\alpha}) = \mathrm{Re}(\sigma(\alpha)), \quad \sigma b = \frac{1}{2\sigma(i)}(\sigma\alpha - \overline{\sigma\alpha}) = \mathrm{Im}(\sigma(\alpha)) \ . \qquad \square$$

Remark 5.2. We recall that a number field L is a CM field if it is a totally complex quadratic extension of a totally real number field. It is well-known (see for instance [29], p. 38) that in a CM field L the complex conjugation defines an involution τ of L which is independent of the embedding into $\mathbb{C}$; i.e. for any $\mathbb{Q}$-embedding $\sigma\colon L \hookrightarrow \mathbb{C}$ we have $\overline{\sigma} = \sigma\tau$. Let $\alpha \in L$. The argument of the proof of Lemma 5.1 shows that

$$a = \frac{1}{2}(\alpha + \tau(\alpha)), \quad b = \frac{1}{2i}(\alpha - \tau(\alpha))$$

are totally real. Thus $\alpha = a + ib \in \mathbb{Q}^{\mathrm{tr}}(i)$. This proves that any CM field is contained in $\mathbb{Q}^{\mathrm{tr}}(i)$ (and actually $\mathbb{Q}^{\mathrm{tr}}(i)$ is the compositum of all CM fields).

We are now in a position to give the promised example.

Theorem 5.3. *The field $\mathbb{Q}^{\mathrm{tr}}$ satisfies (B), but its quadratic extension $\mathbb{Q}^{\mathrm{tr}}(i)$ does not.*

Proof. For the first assertion, see [27] and [28]. For the second one, [3], Theorem 1.3, shows that there exists an infinite sequence (α_k) of algebraic numbers such that the fields $\mathbb{Q}(\alpha_k)$ are CM-fields, α_k is not a root of unity, and $h(\alpha_k) \to 0$. By

Remark 5.2, $\mathbb{Q}(\alpha_k) \subseteq \mathbb{Q}^{\mathrm{tr}}(i)$. Thus the field $\mathbb{Q}^{\mathrm{tr}}(i)$ does not satisfy (B). A more direct example is the following. For $k \in \mathbb{N}$ let

$$\alpha_k = \left(\frac{2-i}{2+i}\right)^{1/k}.$$

Then all the archimedean absolute values of α_k are equal to 1. Thus, by Lemma 5.1, $\alpha_k \in \mathbb{Q}^{\mathrm{tr}}(i)$. Obviously α_k is not a root of unity and $h(\alpha_k) \to 0$ (note, however, that extracting roots is not the only manner to construct a number of small height in $\mathbb{Q}^{\mathrm{tr}}(i)$; see again [3], sections 4 and 5, for details). □

In view of this example, it may not be out of place to study the Galois group of $\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q}$. The *absolute* Galois group of $\mathbb{Q}^{\mathrm{tr}}$ is known. By a result of Freid, Haran and Völklein (see [14]) $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{tr}})$ is freely generated by a subset of involutions homeomorphic to the Cantor set. Nevertheless, nothing is apparently known on $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$.

By a well-known theorem of Artin-Schreier-Baer (see [6] and [7]) the only non-trivial elements of finite order in the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ are the complex conjugations. In the present situation we have:

Theorem 5.4. *There is no automorphism of finite order* > 1 *in* $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$.

We shall give a proof of this theorem in section 7. For the moment, let us reflect on some consequences of this statement.

Let G be a profinite group such that *any* Galois extension $L/\mathbb{Q}$ with Galois group G satisfies (B). Let $L/\mathbb{Q}$ be any such extension. We could ask if any finite extension of L again satisfies (B).

The group $G = \mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$ provides a counterexample to this assertion. Indeed, if $L/\mathbb{Q}$ has Galois group G, then $L \subseteq \mathbb{Q}^{\mathrm{tr}}$. Otherwise we could find an involution in G, contradicting Theorem 5.4. By the quoted result of [27] and [28], any Galois extension $L/\mathbb{Q}$ with Galois group G satisfies (B).

Thus G is a profinite group such that any Galois extension $L/\mathbb{Q}$ with Galois group G satisfies (B). However, as proved in Theorem 5.3, $\mathbb{Q}^{\mathrm{tr}}(i)$ is a quadratic extension of $L = \mathbb{Q}^{\mathrm{tr}}$ which does not satisfy (B) and $\mathrm{Gal}(L/\mathbb{Q}) = G$.

The situation seems to be different if we allow a base change.

Definition 5.5. Let G be a profinite group. We say that G has Property (B) if for any number field K and for any Galois extension L/K with Galois group G, the field L satisfies (B).

By Galois theory, a profinite group G satisfies (B) if and only if *at least one of its subgroups of finite index* satisfies (B). Indeed, let H be a subgroup of finite index of G which satisfies (B). Let L/K be a Galois extension of a number field K such that $\mathrm{Gal}(L/K) = G$. Then L^H is a finite extension of K, hence a number field. Since $\mathrm{Gal}(L/L^H) = H$ satisfies (B), the field L satisfies (B).

We remark that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$ *does not* satisfy (B). Indeed, $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}(i)) \approxeq \mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$ and the field $\mathbb{Q}^{\mathrm{tr}}(i)$ does not satisfy (B).

We also remark that groups G with $G/Z(G)$ of finite exponent satisfy (B), by our main theorem, Theorem 1.5. Moreover, let L/K be a Galois extension of a number field with Galois group abelian or of a finite exponent. Then any finite extension of L again satisfies (B), as we have already seen in the introduction in the special case $K = \mathbb{Q}$.

More generally, let G be a profinite group such that *all its subgroups of finite index* satisfy (B) (this is the case for abelian groups and for groups of finite exponent). Then any finite extension E of a Galois extension L/K of a number field satisfies (B), provided that $\mathrm{Gal}(L/K) = G$. To see this, select a primitive element $\alpha \in E$ over L. Thus $E = L(\alpha)$ and, by Galois theory, $L(\alpha)/K(\alpha)$ is a Galois extension with Galois group isomorphic to $H = \mathrm{Gal}(L/L \cap K(\alpha)) \subseteq G$ of index $[L \cap K(\alpha) : K] \leq [K(\alpha) : K] < \infty$. Since $K(\alpha)$ is a number field, if H satisfies (B), then $L(\alpha)$ satisfies (B).

These remarks suggest the following questions:

Problem 5.6. Let G be a profinite group which satisfies (B).

i) Is it true that any subgroup of G of finite index satisfies (B)?

ii) Let K be a number field and let L/K be a Galois extension with Galois group G. Is it true that any finite extension of L satisfies (B)?

By the remarks above, i) implies ii).

Let $1 \to H \to G' \to G \to 1$ be a group extension of profinite groups. A positive answer to Problem 5.6 ii) would imply that if H is finite and G satisfies (B), then G' satisfies (B). We remark that we cannot replace "H finite" by "H satisfies (B)" in this last statement. Indeed, for p prime the field

$$L = \mathbb{Q}(\mu_{p^\infty}, 2^{1/p}, 2^{1/p^2}, \ldots)$$

obviously does not satisfy (B). However, its Galois group G' over $\mathbb{Q}$ is an extension of a profinite abelian group by another profinite abelian group, thus both satisfying (B) in the sense of Definition 5.5:

$$H = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \approxeq \mathbb{Z}_p^* \qquad \text{and} \qquad G = \mathrm{Gal}(L/\mathbb{Q}(\mu_{p^\infty})) \approxeq \mathbb{Z}_p \ .$$

6. Relations with field arithmetic

In this section we explore some speculative relations between Property (B) and field arithmetic.

We recall that a field K is Pseudo Algebraically Closed (PAC) if each absolutely irreducible variety defined over K has a K-rational point (see [15], chapter 11, for more details). Obviously an algebraically closed field is PAC. We give some evidence for a negative answer to the following problem:

Problem 6.1. Does there exist a PAC field $K \subseteq \overline{\mathbb{Q}}$ which satisfies (B)?

First we remark that algebraic extensions of PAC fields are again PAC fields by a theorem of Ax-Roquette ([15], Corollary 11.2.5). Similarly, if K does not satisfy (B) and if E/K is an algebraic extension, then E does not satisfy (B).

Only a few examples of non-trivial PAC subfields of $\overline{\mathbb{Q}}$ are known. For instance, as a consequence of a deep result of Pop, $\mathbb{Q}^{\mathrm{tr}}(i)$ is a PAC field (see [22], Theorem $\mathfrak{S}$, p. 21, and [17], section 7 before Lemma 7.1). Determining whether or not the maximal solvable extension $\mathbb{Q}^{\mathrm{solve}}$ of $\mathbb{Q}$ is PAC is an open question (see [15], problem 11.5.9 (a)). Observe that both $\mathbb{Q}^{\mathrm{tr}}(i)$ and $\mathbb{Q}^{\mathrm{solve}}$ do not have Property (B). This is obvious for the second field (just add roots of 2), and it is true for the first one by Theorem 5.3.

Another example of a PAC subfield of $\overline{\mathbb{Q}}$ is provided by the compositum $\mathbb{Q}^{\mathrm{symm}}$ of all symmetric extensions of $\mathbb{Q}$ (i.e. of all Galois extensions over $\mathbb{Q}$ with Galois group a symmetric group); see [15], Th. 18.10.4. Again, this field does not satisfy

(B). To prove this statement, it is enough to find a family L_1, L_2, ... of symmetric extensions of $\mathbb{Q}$ such that

$$\lim_{n\to+\infty} \inf\{h(\alpha) \mid \alpha \in L_n,\ \alpha \text{ not a root of unity}\} = 0\ .$$

We can choose for $\{L_n\}$ the set of splitting fields of $x^p + x + 1$ for $p > 3$ prime, $p \not\equiv 1 \bmod 4$. Indeed if p is prime, x^p+x+1 is irreducible, and if p satisfies the said condition, its splitting field is a symmetric extension (see [18]). Moreover, let α be a root of x^p+x+1. Then α is not a root of unity and $ph(\alpha) = h(\alpha+1) \leq h(\alpha)+\log 2$ by well-known properties of Weil's height. Thus $h(\alpha) \leq (\log 2)/(p-1) \to 0$ as $p \to +\infty$.

The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a compact group and thus admits a translation invariant Haar measure. Let $e \in \mathbb{N}$. By a theorem of Jarden (*PAC Nullstellensatz*; see [15], Th. 18.6.1), for almost all $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^e$ the field $\overline{\mathbb{Q}}^{\boldsymbol{\sigma}}$ fixed by $\sigma_1, \ldots, \sigma_e$ is PAC. It is again quite simple to prove that *any* such field does not satisfy (B):

Proposition 6.2. *Let H be a finitely generated subgroup H of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\overline{\mathbb{Q}}^H$ does not satisfy (B).*

Proof. Let $\sigma_1, \ldots, \sigma_e$ be generators of H. We fix a positive integer N. For $n \in \mathbb{N}$ we have $\sigma_i n^{1/N} = \zeta_N^{a_{i,n}} n^{1/N}$ for some $a_{i,n} \in \mathbb{Z}$, $0 \leq a_{i,n} < N$. By the box principle, there exist n_1, n_2 with $1 \leq n_1 < n_2 \leq N^e+1$ such that $a_{i,n_1} = a_{i,n_2}$ for $i = 1, \ldots, e$. Thus $\alpha_N := (n_1/n_2)^{1/N}$ is fixed by all σ_i; henceforth it is in $\overline{\mathbb{Q}}^H$. We have

$$0 < h(\alpha_N) = \frac{h(n_1/n_2)}{N} \leq \frac{2\log(N^e+1)}{N} \to 0$$

as $N \to \infty$. This shows that $\overline{\mathbb{Q}}^H$ does not satisfy (B). □

Another central definition in field arithmetic is the Hilbertianity. A field K is Hilbertian if it satisfies Hilbert's Irreduciblity Theorem: for every irreducible $f \in K[x, y]$ which is separable in x there exists $a \in K$ such that $f(x, a)$ is irreducible over K (see [15], chapter 12, for more details). As for PAC fields, we could ask for relations between Hilbertianity and (B). But now, we do not have any direct implication. Indeed $\mathbb{Q}^{\mathrm{tr}}$ is not Hilbertian (choose $f(x, y) = x^2 - y^2 - 1$) and satisfies (B); on the contrary $\mathbb{Q}^{\mathrm{tr}}(i)$ is Hilbertian (by Weissauer's Theorem, [15], chapter 13, Theorem 13.9.1) and does not satisfy (B). Another example of field with these properties is $\mathbb{Q}^{\mathrm{symm}}$, which is Hilbertian (see [15], Theorem 18.10.4) and does not satisfy (B), as already remarked.

7. On the Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$

The field $\mathbb{Q}^{\mathrm{tr}}$ has a subset of *totally positive* elements, i.e. those all of whose conjugates are non-negative. We shall repeatedly use the easy observation that:

A square root of a totally positive element lies in $\mathbb{Q}^{\mathrm{tr}}$.

Indeed, if α is totally positive and $\beta^2 = \alpha$, we have $(\sigma\beta)^2 = \sigma\alpha$, which is real and ≥ 0 for every $\mathbb{Q}$-embedding $\sigma\colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$; hence $\sigma\beta \in \mathbb{R}$ for each such σ, as asserted.

We shall now prove Theorem 5.4. Let σ be a non-trivial $\mathbb{Q}$-automorphism of finite order of the field of totally real algebraic numbers. By replacing σ with a power of

it, we may suppose that its order is a prime l. We shall derive a contradiction. Let us start with the

Case $l = 2$. Since σ is supposed to have order 2, its fixed field F is such that $[\mathbb{Q}^{\mathrm{tr}} : F] = 2$. We have $\mathbb{Q}^{\mathrm{tr}} = F(\beta)$ for a β such that $\alpha := \beta^2 \in F$.

We shall use the following:

Lemma 7.1. *The number α is a sum of two squares of elements of F.*

Proof. We shall use a result of Hilbert and Landau (see [19], Exercise 1, p. 461, or [23], Theorem 15.11, p. 224): a totally positive α is a sum of squares in $\mathbb{Q}(\alpha)$. In the Appendix below we shall give a self-contained proof of this result (Theorem 8.1).

Note that since β is totally real, α is totally positive. By the quoted result, α is then a sum of squares in $\mathbb{Q}(\alpha)$, hence in F. Let $\alpha = a_1^2 + \ldots + a_m^2$, $a_1, \ldots, a_m \in F$, be such a representation with minimal m. If $m \geq 2$, let $\xi := a_1^2 + \ldots + a_{m-1}^2$. Since the a_i lie in $\mathbb{Q}^{\mathrm{tr}}$, we have that ξ is totally positive. Hence $\sqrt{\xi}$ is totally real; i.e. there exists $\mu \in \mathbb{Q}^{\mathrm{tr}}$ with $\mu^2 = \xi$. We can write $\mu = p + \beta q$ with $p, q \in F$, and then $\xi = p^2 + \alpha q^2 + 2pq\beta$. Since $\xi \in F$ we must have $pq = 0$, but of course we may assume that p, q do not both vanish. If $p = 0$, then $q \neq 0$, and we obtain a representation of α as a sum of $m - 1$ squares, a contradiction. Then $q = 0$. But then $\xi = p^2$ and $\alpha = p^2 + a_m^2$, as required. □

By Lemma 7.1, we may find $x, y \in F^*$ such that $x^2 - \alpha y^2 = -1$. Set $\gamma := x + \beta y$, so $N(\gamma) = -1$, where N is the norm from $\mathbb{Q}^{\mathrm{tr}}$ to F.

We have $N(\gamma^2) = 1$. Set $\eta := 1 + \gamma^2$, and denote with an accent the said automorphism (i.e. the conjugation of $\mathbb{Q}^{\mathrm{tr}}$ over F). We have $\gamma^2(\gamma')^2 = 1$, so $\eta' = 1 + (\gamma')^2 = 1 + \gamma^{-2} = \eta\gamma^{-2}$.

Since $\gamma \in \mathbb{Q}^{\mathrm{tr}}$, the element η is totally positive, whence $\eta = \delta^2$ for some $\delta \in (\mathbb{Q}^{\mathrm{tr}})^*$. Hence $\gamma^2(\delta')^2 = \delta^2$, leading to $\gamma = \pm\delta/\delta'$. But then $N(\gamma) = 1$, and we have a contradiction, concluding the proof in the case $l = 2$.

As pointed out by B. Deschamps, a more direct proof in Case $l = 2$ follows from a result of Diller and Dress (see [26], Ch. IX, §7, and [23]) on Pythagorean fields.

Case $l > 2$. We recall that $\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}$ is also Galois as the composite of the Galois extensions $\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q}$ and $\mathbb{Q}(i)/\mathbb{Q}$. Note that $\mathbb{Q}^{\mathrm{tr}}(i)$ contains all roots of unity (as an immediate consequence of Lemma 5.1). We also recall that the complex conjugation of $\mathbb{C}$ defines an automorphism τ of $\mathbb{Q}^{\mathrm{tr}}(i)$ which is independent of the embedding into $\mathbb{C}$. By abuse of notation, we shall denote this automorphism by the usual symbol $\overline{\alpha} := \tau(\alpha)$.

Let L denote the fixed field of σ in $\mathbb{Q}^{\mathrm{tr}}$; we may extend σ to an automorphism, again denoted σ, of $\mathbb{Q}^{\mathrm{tr}}(i)$, fixing i so $L(i)$ is the fixed field of σ in $\mathbb{Q}^{\mathrm{tr}}(i)$ and $[\mathbb{Q}^{\mathrm{tr}}(i) : L(i)] = [\mathbb{Q}^{\mathrm{tr}} : L] = l$. Note that $\mathbb{Q}^{\mathrm{tr}}(i)$ contains the l-th roots of unity, whose degree over $L(i)$ divides $l - 1$, but this degree also divides l, whence $L(i)$ contains the l-th roots of unity. By Kummer's theory we then have $\mathbb{Q}^{\mathrm{tr}}(i) = L(i)(\beta)$ where $\beta^l =: \alpha \in L(i)$ and $\sigma(\beta) = \theta\beta$ for some primitive l-th root of unity θ. Since $L \subset \mathbb{Q}^{\mathrm{tr}}$, $L(i)$ is sent into itself by complex conjugation, so also $\overline{\beta}$ generates $\mathbb{Q}^{\mathrm{tr}}(i)$ over $L(i)$ and $\overline{\beta}^l = \overline{\alpha} \in L(i)$. By Kummer's theory again, we have

$$\overline{\beta} = \gamma\beta^r, \qquad \gamma \in L(i)\,, \tag{7.1}$$

for some r coprime to l (only its residue class mod l matters in (7.1)).

Applying to (7.1) complex conjugation we get $\beta = \overline{\gamma}\overline{\beta}^r$, and using (7.1) in this last equation we obtain

$$\beta = \overline{\gamma}\gamma^r\beta^{r^2},$$

whence $\beta^{r^2-1} \in L(i)$. Since $\beta^l \in L(i)$ and β is not in $L(i)$, this yields $r^2 \equiv 1 \pmod{l}$, so $r \equiv \pm 1 \pmod{l}$. Then we may suppose $r = \pm 1$ in (7.1), so also $\overline{\gamma}\gamma^r = 1$.

If $r = 1$ we have $\overline{\gamma}\gamma = 1$, whence (by Hilbert 90 for $L(i)/L$) $\gamma = u/\overline{u}$ for some $u \in L(i)$. Then $\overline{u\beta} = u\beta$, so $u\beta$ is totally real, and then $u\beta \in \mathbb{Q}^{\mathrm{tr}}$. But since σ fixes $L(i)$ pointwise and stabilizes $\mathbb{Q}^{\mathrm{tr}}$, this contradicts that $\sigma(\beta)/\beta$ is a primitive l-th root of unity, so is not totally real.

Therefore we have $r = -1$ and $\beta\overline{\beta} = \gamma \in L(i)$ (actually $\gamma \in L$ since this shows it is totally real).

Note now that $\mathbb{Q}^{\mathrm{tr}}(i) = L(i)(\rho\beta^s)$ for every $\rho \in L(i)^*$ and every s coprime to l; hence we may replace β with such $\rho\beta^s$ to generate $\mathbb{Q}^{\mathrm{tr}}(i)/L(i)$. We choose $s = 2$ and $\rho = (\beta\overline{\beta})^{-1}$, so $\rho\beta^s = \beta/\overline{\beta} =: \xi$, say, and $\mathbb{Q}^{\mathrm{tr}}(i) = L(i)(\xi)$, where $\mu := \xi^l = \beta^{2l}/\gamma^l \in L(i)$.

All conjugates of ξ have absolute value 1, so all the conjugates of $\xi^{\frac{1}{l}}$ have absolute value 1, and therefore, by Lemma 5.1, $\xi^{\frac{1}{l}}$ lies in $\mathbb{Q}^{\mathrm{tr}}(i)$ for every choice of the l-th root. Note that $(\xi^{\frac{1}{l}})^{l^2} = \xi^l = \mu$.

At this point the proof mimics an argument of Artin, proving that $\mathbb{C}$ has no automorphisms of finite odd order (see [19], p. 299, Cor. 9.3). The polynomial $x^{l^2} - \mu = x^{l^2} - \xi^l$ lies in $L(i)[x]$ and has a root (actually all roots) in $\mathbb{Q}^{\mathrm{tr}}(i)$. But $[\mathbb{Q}^{\mathrm{tr}}(i) : L(i)] = l$, so the polynomial is reducible. By Capelli's Theorem (see [19], Ch. VIII, Theorem 16), we have $\mu = a^l$ for some $a \in L(i)$. This yields $\xi = \zeta a$ for an l-th root of unity ζ, and since ζ lies in $L(i)$ as noted above, we deduce that $\xi \in L(i)$, a contradiction which proves the theorem. □

8. Appendix

In this Appendix we provide a self-contained proof of the following result, used in the proof of Lemma 7.1:

Theorem 8.1. *Let α be a totally real algebraic number. Then an element of $\mathbb{Q}(\alpha)$ is a sum of squares in $\mathbb{Q}(\alpha)$ if and only if it is totally positive.*

Proof. This theorem is due to Hilbert and Landau, in a more general form when α is not necessarily totally real, and it is required that all embeddings in $\mathbb{R}$ of the relevant number are positive. See Lang's ([19]) or Rajwade's ([23]) above-quoted references for a proof which depends on Artin-Schreier's theory of real fields. The simple proof below is independent of this theory and would seemingly work with small modifications also for the more general assertion.

To prove Theorem 8.1 note that one half of the conclusion is clear, and so it suffices to work on the assumption that α is totally positive and to prove that α is a sum of squares in $\mathbb{Q}(\alpha)$.

We let $d := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and we denote by $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ the (positive) distinct conjugates of α over $\mathbb{Q}$.

There are polynomials $f_1, \ldots, f_d \in \mathbb{R}[x]$ of degree at most $d-1$ and such that $f_i(\alpha_j)$ equals 2 if $i = j$ and 0 otherwise (just solve a Vandermonde linear system or else take $f_i(x) = c_i \prod_{r \neq i}(x - \alpha_r)$ with $c_i = 2\prod_{r\neq i}(\alpha_i - \alpha_r)^{-1}$). Let us choose $\epsilon > 0$

as a real positive number $< \frac{\min \alpha_i}{2d \max \alpha_i}$. By approximating the coefficients of f_i with rational numbers and squaring, we may then find polynomials $g_1, \dots, g_d \in \mathbb{Q}[x]$ (also of degree $\leq d-1$) such that, for $i = 1, \dots, d$,

$$g_i^2(\alpha_i) > 1, \qquad g_i^2(\alpha_j) < \epsilon, \quad j \neq i. \tag{8.1}$$

Define vectors $v_1, \dots, v_d \in \mathbb{R}^d$ by

$$v_i := (g_1^2(\alpha_i), \dots, g_d^2(\alpha_i)).$$

Note that $v_1, \dots, v_d$ are $\mathbb{R}$-linearly independent: if $t_1 v_1 + \dots + t_d v_d = 0$ with real t_i not all 0, we may assume by dividing by a coefficient of maximal absolute value that $t_r = 1$ for some $1 \leq r \leq d$, while $|t_i| \leq 1$ for $i = 1, \dots, d$. The relation implies $t_1 g_r^2(\alpha_1) + \dots + t_d g_r^2(\alpha_d) = 0$, whence $1 < g_r^2(\alpha_r) \leq (d-1)\epsilon$, a contradiction with the said choice of ϵ.

Then we may find (uniquely!) real numbers $c_1, \dots, c_d$ such that

$$\alpha_i = c_1 g_1^2(\alpha_i) + \dots + c_d g_d^2(\alpha_i), \qquad i = 1, \dots, d. \tag{8.2}$$

The c_i are surely in $\mathbb{Q}(\alpha_1, \dots, \alpha_d)$ but must actually be in $\mathbb{Q}$, as can be seen by uniqueness and taking conjugates of these relations or also directly by noting that the independence of the v_i amounts to the fact that $g_1^2(\alpha), \dots, g_d^2(\alpha)$ is a basis of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

We contend that $c_i \geq 0$ for all i. Indeed, let $M := \max |c_i|$ and suppose that $M = |c_r|$. Evaluating (8.2) at $i = r$ and recalling (8.1) we have

$$M \leq \epsilon(d-1)M + |\alpha_r| \leq M/2 + \max |\alpha_i|,$$

proving that $M \leq 2 \max |\alpha_i|$. Now, suppose by contradiction that $c_s < 0$, and evaluate (8.1) at $i = s$. We obtain

$$0 < \alpha_s \leq \sum_{j \neq s} c_j g_j^2(\alpha_s) \leq M(d-1)\epsilon \leq 2(d-1)(\max |\alpha_i|)\epsilon \ .$$

But this contradicts our choice of ϵ.

Then the c_i are non-negative rationals, and therefore each of them is a sum of squares of rational numbers: for a, b positive integers, the fraction $\frac{a}{b}$ is the sum of ab equal squares $\frac{1}{b^2}$. Then, relation (8.2) for $i = 1$ proves the sought-after conclusion. □

Remark 8.2. Note that the proof shows that only d distinct squares (each repeated a suitable number of times) suffice to represent α in the sought-after shape.

Acknowledgements

The authors are indebted to P. Dèbes, B. Deschamps and M. Fried for useful discussions on the subject of sections 6 and 7. They also thank D. Simon, who provided them with reference [18].

References

[1] Francesco Amoroso and Sinnou David, *Minoration de la hauteur normalisée dans un tore*, J. Inst. Math. Jussieu **2** (2003), no. 3, 335–381 (French, with English and French summaries), DOI 10.1017/S1474748003000094. MR1990219 (2004m:11101)

[2] Francesco Amoroso and Roberto Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), no. 2, 260–272, DOI 10.1006/jnth.1999.2451. MR1740514 (2001b:11100)

[3] Francesco Amoroso and Filippo A. E. Nuccio, *Algebraic numbers of small Weil's height in CM-fields: on a theorem of Schinzel*, J. Number Theory **122** (2007), no. 1, 247–260, DOI 10.1016/j.jnt.2006.04.005. MR2287122 (2007i:11088)

[4] Francesco Amoroso and Umberto Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29** (2000), no. 3, 711–727. MR1817715 (2003a:11078)

[5] Francesco Amoroso and Umberto Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*, Bull. Lond. Math. Soc. **42** (2010), no. 3, 489–498, DOI 10.1112/blms/bdq008. MR2651944 (2011k:11157)

[6] E. Artin and O. Schreier, "Algebraische Konstruktion reeller Körper", pp. 258–272 in: Artin's Collected Papers (Ed. S. Lang and J. Tate), Springer-Verlag, New York, 1982. MR0671416 (83j:01083)

[7] Reihold Baer, *Die Automorphismengruppe eines algebraisch abgeschlossenen Körpers der Charakterkistik* 0 (German), Math. Z. **117** (1970), 7–17. MR0272757 (42 #7638)

[8] Matthew H. Baker and Joseph H. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett. **11** (2004), no. 2-3, 377–396. MR2067482 (2005e:11083)

[9] Enrico Bombieri and Umberto Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$ (English, with English and Italian summaries), Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **12** (2001), 5–14 (2002). MR1898444 (2003d:11155)

[10] S. Checcoli, "Fields of algebraic numbers with bounded local degrees and their properties", Trans. Amer. Math. Soc. **365** (2013), no. 4, 2223–2240. MR3009657

[11] Sinnou David and Amílcar Pacheco, *Le problème de Lehmer abélien pour un module de Drinfel'd*, Int. J. Number Theory **4** (2008), no. 6, 1043–1067 (French, with English and French summaries), DOI 10.1142/S1793042108001870. MR2483311 (2010d:11061)

[12] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401. MR543210 (80i:10040)

[13] Roberto Dvornicich and Umberto Zannier, *On the properties of Northcott and of Narkiewicz for fields of algebraic numbers*, Funct. Approx. Comment. Math. **39** (2008), part 1, 163–173, DOI 10.7169/facm/1229696562. MR2490096 (2009k:11170)

[14] Michael D. Fried, Dan Haran, and Helmut Völklein, *Absolute Galois group of the totally real numbers* (English, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 11, 995–999. MR1249777 (94k:12007)

[15] Michael D. Fried and Moshe Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden. MR2445111 (2009j:12007)

[16] P. Habegger, *Small height and infinite non-Abelian extensions*, Duke Math. J. **162** (2013), no. 11, 2027–2076.

[17] Moshe Jarden and Aharon Razon, *Pseudo algebraically closed fields over rings*, Israel J. Math. **86** (1994), no. 1-3, 25–59, DOI 10.1007/BF02773673. MR1276130 (95c:12006)

[18] Kenzo Komatsu, *On the Galois group of* $x^p + ax + a = 0$, Tokyo J. Math. **14** (1991), no. 1, 227–229, DOI 10.3836/tjm/1270130502. MR1108169 (92e:11127)

[19] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556 (2003e:00003)

[20] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), no. 3, 461–479, DOI 10.2307/1968172. MR1503118

[21] Patrice Philippon and Martín Sombra, *Minimum essentiel et degrés d'obstruction des translatés de sous-tores*, Acta Arith. **133** (2008), no. 1, 1–24 (French), DOI 10.4064/aa133-1-1. MR2413362 (2009g:11079)

[22] Florian Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), no. 1, 1–34, DOI 10.2307/2118581. MR1405941 (97h:12013)

[23] A. R. Rajwade, *Squares*, London Mathematical Society Lecture Note Series, vol. 171, Cambridge University Press, Cambridge, 1993. MR1253071 (94m:11047)

[24] Nicolas Ratazzi, *Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe*, Int. Math. Res. Not. **58** (2004), 3121–3152 (French), DOI 10.1155/S1073792804140518. MR2098701 (2005k:11116)

[25] G. Rémond, Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink, to appear, *Séminaires et congrès*.
[26] Paulo Ribenboim, *L'arithmétique des corps* (French), Hermann, Paris, 1972. MR0330093 (48 #8432)
[27] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday. IV, Acta Arith. **24** (1973), 385–399. MR0360515 (50 #12963)
[28] C. J. Smyth, *On the measure of totally real algebraic integers*, J. Austral. Math. Soc. Ser. A **30** (1980/81), no. 2, 137–149. MR607924 (82j:12002a)
[29] Lawrence C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982. MR718674 (85g:11001)

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

Institut de Mathématiques, CNRS UMR 7586, Université Pierre et Marie Curie, 4, place Jussieu, 75252 Paris Cedex 05, France

Scuola Normale Superiore, Piazza dei Cavalieri, 56126 Pisa, Italy