

HEIGHT LOWER BOUNDS FOR ELEMENTS OF HIGHLY COMPOSITE RINGS

SIU HANG MAN, NICLAS TECHNAU, MARTIN WIDMER, AND PAVLO YATSYNA

ABSTRACT. Let $\mathbb{Q}^{(d)}$ be the composite field of all number fields of degree at most d . In 2001 Bombieri and Zannier proved that $\mathbb{Q}^{(2)}$ has the Northcott property and asked what happens for $d \geq 3$. Here we study the absolute Weil height for elements in the composite ring of the rings of integers of such number fields. In particular, we consider $\mathbb{Q}^{(3)}$ as the composite field of $\mathbb{Q}^{(2)}$ and a minimal infinite family of cubic fields, and we show that the composite ring of the rings of integers of these fields does have the Northcott property. Our results follow from new height lower bounds, expressed in terms of the degree. Moreover, we introduce a notion of size for subfields of $\mathbb{Q}^{(3)}$. For instance, $\mathbb{Q}^{(3)}$ has size 1 and the maximal abelian subfield of $\mathbb{Q}^{(3)}$ has size $1/2$. We show that there is a subfield of $\mathbb{Q}^{(3)}$ of size 1 which has the Northcott property.

1. INTRODUCTION

Let K be a number field. For each place v of K we choose the unique representative $|\cdot|_v$ that either extends the usual archimedean absolute value or one of the usual p -adic absolute values on $\mathbb{Q}$. We write K_v for the completion of K at v and we write $d_v = [K_v : \mathbb{Q}_v]$ for the local degree at v . For $\alpha \in K$ we define the absolute multiplicative Weil height by

$$(1.1) \quad H(\alpha) = \prod_v \max \{1, |\alpha|_v\}^{\frac{d_v}{[K:\mathbb{Q}]}} ,$$

where the product runs over all places v of K . Taking the $[K : \mathbb{Q}]$ -th root in the above definition makes the height independent of the particular choice of the field K containing α (see [4, Lemma 1.5.2]). Hence the height defines a genuine function on the algebraic numbers $\overline{\mathbb{Q}}$. We write $h(\alpha) = \log H(\alpha)$ for the logarithmic Weil height of α . For more details on the Weil height we refer the reader to [4, Section 1.5].

We are interested in bounding the height of elements of a specific subset $R \subset \overline{\mathbb{Q}}$ from below in terms of their degrees. The question is of particular interest when R is a subring or subfield of $\overline{\mathbb{Q}}$. By Kronecker's theorem $h(\alpha) = 0$ if and only if α is a root of unity or zero. We are excluding these cases throughout our discussion. Lehmer's conjecture from 1933 asserts that

$$(1.2) \quad h(\alpha) \geq \frac{c_0}{[Q(\alpha) : \mathbb{Q}]}$$

for some absolute constant $c_0 > 0$. If $Q(\alpha)/\mathbb{Q}$ is Galois, then (1.2) holds by a result of Amoroso and David [1]. The latter was improved by Amoroso and Masser [3] to

$$(1.3) \quad h(\alpha) \geq \frac{c_\varepsilon}{[Q(\alpha) : \mathbb{Q}]^\varepsilon}$$

for any $\varepsilon > 0$. Assuming $Q(\alpha)/\mathbb{Q}$ is abelian, one even has an absolute lower bound

$$(1.4) \quad h(\alpha) \geq \frac{\log 5}{12}$$

by an older result of Amoroso and Dvornicich [2]. Let $\mathbb{Q}^{(d)}$ be the composite field of all number fields of degree at most d . Bombieri and Zannier [5] showed that there exists a nondecreasing *unbounded* function $F : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{R}_{\geq 0}$, (depending on d) such that

$$(1.5) \quad h(\alpha) \geq F([Q(\alpha) : \mathbb{Q}])$$

whenever $Q(\alpha)/\mathbb{Q}$ is abelian and contained in $\mathbb{Q}^{(d)}$.

We say a set $S \subset \overline{\mathbb{Q}}$ has property (1.5) if there exists a nondecreasing *unbounded* function $F : \mathbb{Z}_{\geq 1} \rightarrow \mathbb{R}_{\geq 0}$, such that (1.5) holds for all $\alpha \in S^*$, where S^* is the subset of S deprived by 0 and all roots of unity. Property (1.5)

Date: August 12, 2026.

2020 Mathematics Subject Classification. 11G50, 11R04.

Key words and phrases. Algebraic number theory, Weil height, Northcott property, Lehmer's conjecture.

S.H.M. and P.Y. were supported by the Czech Science Foundation GAČR grant 26-20514S. S.H.M. was supported by the Charles University programme PRIMUS/25/SCI/008. N.T. was supported by the University of Wisconsin–Madison, Office of the Vice Chancellor for Research with funding from the Wisconsin Alumni Research Foundation. During the early stages of this project, N.T. was supported by a Schrödinger Fellowship of the Austrian Science Fund (FWF): project J 4464-N. P.Y. was supported by the Charles University programme PRIMUS/24/SCI/010.

is essentially a reformulation of the following important finiteness property, formally introduced by Bombieri and Zannier [5] in 2001.

Definition 1 (Bombieri, Zannier [5]). *A set $S \subset \overline{\mathbb{Q}}$ has the Northcott property if $\#\{\alpha \in S : h(\alpha) \leq X\} < \infty$ for every $X \geq 0$. For brevity, we say that S has (N) to express that S has the Northcott property.*

The Northcott property has many applications (diophantine and beyond) and has been studied intensively over the last 25 years, see, e.g., [21] for a survey. But its origin goes back to 1950 when Northcott (see [14] and also [4, Theorem 1.6.8]) showed that sets of uniformly bounded degree have (N).

Thanks to Northcott's Theorem the precise relation between property (1.5) and (N) is now clear. A set S has (N) if and only if it has only finitely many roots of unity and has property (1.5). A set which contains infinitely many roots of unity and is closed under addition contains an infinite sequence (without roots of unity) with uniformly bounded height¹, hence cannot have property (1.5). Consequently, for sets that are closed under addition properties (N) and (1.5) are equivalent.

Since the maximal abelian subfield $\mathbb{Q}_{ab}^{(d)}$ of $\mathbb{Q}^{(d)}$ coincides with $\mathbb{Q}^{(d)}$ when $d = 2$ we know that $\mathbb{Q}^{(2)}$ has (N). Bombieri and Zannier asked the following question.

Question 1 (Bombieri, Zannier, [5]). *Does a bound as in (1.5) hold for $\mathbb{Q}^{(d)}$ when $d \geq 3$?*

In other words, does $\mathbb{Q}^{(d)}$ have (N)? The case $d = 3$ is already widely open and presents a major challenge. In this article we will focus on $d = 3$, albeit some of our results are more general.

We think of $\mathbb{Q}^{(3)}$ as the compositum of $L_0 = \mathbb{Q}^{(2)}$ and an infinite sequence of cubic fields $K_1, K_2, K_3, \dots$. We can assume that the compositum $L_n = L_{n-1}K_n$ is a proper extension of L_{n-1} for every n . We are unable to prove that the elements of

$$\mathbb{Q}^{(3)} = L_0 \prod_n K_n$$

satisfy the required height lower bound but we show that such a height lower bound exists for the composite ring of integers of these fields, i.e., for

$$(1.6) \quad \mathcal{O}_{L_0} \prod_{n=1}^{\infty} \mathcal{O}_{K_n}.$$

The above claim follows from Corollary 1 (see paragraph after Corollary 1).

The following notation and definitions are assumed throughout this article.

Definition 2.

(a) For a field $K \subseteq \overline{\mathbb{Q}}$, let $\mathcal{O}_K$ be its ring of integers. For a family S_i ($i \in \mathcal{I} \subset \mathbb{N}$) of subrings of $\overline{\mathbb{Q}}$, we write

$$\prod_{i \in \mathcal{I}} S_i$$

for the composite ring, i.e., the smallest subring of $\overline{\mathbb{Q}}$ containing S_i for each $i \in \mathcal{I}$.

(b) L_0 denotes a subfield of $\overline{\mathbb{Q}}$, and $(K_i)_i$ is a sequence of number fields of respective degrees $d_i = [K_i : \mathbb{Q}] > 1$. We write

$$(1.7) \quad L_n = L_0 \prod_{i=1}^n K_i, \quad R_n = \mathcal{O}_{L_0} \prod_{i=1}^n \mathcal{O}_{K_i}$$

for the composite rings. Note that the former is a field.² We denote the composite ring of all R_n by

$$R = \bigcup_n R_n.$$

(c) We say the family $L_0, K_1, K_2, K_3, \dots$ is linearly disjoint over $\mathbb{Q}$ if every finite subfamily is linearly disjoint over $\mathbb{Q}$.

Remark 1. The linear disjointness of $L_0, K_1, K_2, K_3, \dots$ over $\mathbb{Q}$ is equivalent to $[L_n : L_{n-1}] = [K_n : \mathbb{Q}]$ for every $n \in \mathbb{N}$ (see [10] discussion before Lemma 2.5.6).

It is slightly more convenient to prove and express the results in terms of the multiplicative height $H(\cdot)$ defined in (1.1).

Theorem 1. Suppose the family $L_0, K_1, K_2, K_3, \dots$ is linearly disjoint over $\mathbb{Q}$, and all degrees d_i are prime and bounded from above by some $d \in \mathbb{N}$. Then there exists $c_d > 0$, depending only on d , such that for every $\alpha \in R$

$$(1.8) \quad H(\alpha) \geq c_d (\log[L_0(\alpha) : L_0])^{\frac{1}{d^3}}.$$

¹This follows from the general inequality $h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2$.

²This follows from the fact that if $K \subset \overline{\mathbb{Q}}$ is a field and $\beta_1, \dots, \beta_n \in \overline{\mathbb{Q}}$ then $K[\beta_1, \dots, \beta_n] = K(\beta_1, \dots, \beta_n)$.

Apart from the choice of L_0 and d the height lower bound (1.8) is completely independent of the particular choice of the ring R . For each L_0 and $d > 1$ let us define $\mathcal{R}_{L_0}(d)$ to be the union of all rings R as in Definition 2 (b) that are satisfying the hypothesis of Theorem 1. Hence, the height bound (1.8) remains valid for every element $\alpha \in \mathcal{R}_{L_0}(d)$. Unfortunately, $\mathcal{R}_{L_0}(d)$ need not be a ring in general.

If the Galois closures of the fields $L_0, K_1, K_2, K_3, \dots$ are also linearly disjoint over $\mathbb{Q}$ then the condition that the degrees d_i be prime in Theorem 1 can be replaced by the weaker constraint L_i/L_{i-1} has no proper intermediate field. We will explain this more thoroughly in Section 4.

In the spirit of Lehmer one can ask what is the correct dependence on the degree $[L_0(\alpha_n) : L_0]$ of the lower bound (1.8)? Here is a simple upper bound for $L_0 = \mathbb{Q}$ and $K_i = \mathbb{Q}(p_i^{1/d})$, where d is a prime and p_i is the i -th prime. Taking $\alpha_n = \sum_{i=1}^n p_i^{1/d} \in R$, and estimating its height by the maximal modulus of the conjugates gives $H(\alpha_n) \leq n(n \log n)^{1/d} \leq n^{1.01+1/d}$ (assuming n is big enough). As the degree of α_n is given by d^n we conclude

$$(1.9) \quad H(\alpha_n) \leq (\log[L_0(\alpha_n) : L_0])^{1.01+1/d}.$$

So here the correct exponent lies between $1/d^3$ and $1.01 + 1/d$. Using that for most conjugates of α_n there is much cancellation one can easily reduce the exponent $1.01 + 1/d$ in (1.9). And it is also clear from the proof of Theorem 1 that the exponent $1/d^3$ is far from sharp and can easily be improved. However, finding the sharp exponent of the lower bound in (1.8) seems a rather challenging problem, even when $L_0 = \mathbb{Q}$ and $d = 2$.

Theorem 1 is an immediate consequence of the following result. Recall that we are assuming $d_i > 1$ for all $i \in \mathbb{N}$ throughout.

Theorem 2. *Suppose the family $L_0, K_1, K_2, K_3, \dots$ is linearly disjoint over $\mathbb{Q}$ and that there exists $d > 1$ so that $d_i = [K_i : \mathbb{Q}] \leq d$ for all $i \in \mathbb{N}$. If $\alpha \in R$ and $L_{m-1}(\alpha) = L_m$, then*

$$(1.10) \quad H(\alpha) \geq c_d |\Delta_{K_m}|^{\frac{1}{2d_m(d_m-1)}}$$

for some $c_d > 0$ depending only on d .

Before we proceed, let us deduce Theorem 1 from Theorem 2.

Proof of Theorem 1 assuming Theorem 2. First we reorder the fields K_i such that the discriminants $|\Delta_{K_i}|$ are increasing. Clearly, this does not affect the linear disjointness of the family $L_0, K_1, K_2, K_3, \dots$ but we get a new sequence of fields $(L_i)_i$. Suppose $\alpha \in L_m \setminus L_{m-1}$. The linear disjointness gives $[L_m : L_{m-1}] = [K_m : \mathbb{Q}] = d_m$. Since d_m is assumed to be prime, we conclude that $L_{m-1}(\alpha) = L_m$. Further, $[L_0(\alpha) : L_0] \leq [L_m : L_0] \leq d^m$. Using the very crude bound that among m number fields of degree $\leq d$ there must be at least one with discriminant $\gg_d m^{2/d}$ we conclude

$$H(\alpha) \gg_d m^{\frac{2}{2d_m(d_m-1)d}} \gg_d (\log[L_0(\alpha) : L_0])^{\frac{1}{d^3}},$$

as required. $\square$

To compare (1.10) with bounds from the literature let us assume the ground field L_0 is a number field. Mahler's classical bound applies to any algebraic integer α . Let D be its degree and $f_{\alpha/\mathbb{Q}}$ its minimal polynomial over $\mathbb{Q}$, then

$$H(\alpha) \geq D^{-1/D} |\text{disc}(f_{\alpha/\mathbb{Q}})|^{\frac{1}{2D(D-1)}}.$$

Dixit and Kala [8, Section 3.1] have generalized Mahler's inequality from $\mathbb{Q}$ to arbitrary ground fields. To relate their bound with (1.10) let us briefly sketch the idea behind the proof of Theorem 2. Let $\alpha \in R$ and $L_{m-1}(\alpha) = L_m$. For simplicity let us additionally assume $\alpha \in R_m$. First we express the discriminant of $f_{\alpha/L_{m-1}}$ in terms of the discriminant of K_m . Choosing an integral generator θ_m of K_m one can show³

$$(1.11) \quad \text{disc}(f_{\alpha/L_{m-1}}) = \Delta_{\mathbb{Z}[\theta_m]} \frac{B^2}{I_m^{d_m(d_m-1)}} = \Delta_{K_m} \frac{B^2}{I_m^{d_m(d_m-1)-2}}$$

where I_m is the index $[\mathcal{O}_{K_m} : \mathbb{Z}[\theta_m]]$ and B is some non-zero algebraic integer over which we have little control. Now Dixit and Kala's relative Mahler measure inequality [8, (6)] gives

$$(1.12) \quad H(\alpha) \geq d_m^{-\frac{1}{d_m}} |N_{L_{m-1}/\mathbb{Q}}(\text{disc}(f_{\alpha/L_{m-1}}))|^{\frac{1}{2[L_{m-1}:\mathbb{Q}]d_m(d_m-1)}}.$$

For our bound (1.10) the contribution of B^2 to the height has been ignored. Doing the same here and combining (1.11) and (1.12) gives

$$H(\alpha) \geq d_m^{-\frac{1}{d_m}} \left(\frac{\Delta_{K_m}}{I_m^{d_m(d_m-1)-2}} \right)^{\frac{1}{2d_m(d_m-1)}}.$$

³Apply Lemma 1 and use that $R_m \subset (1/I_m)R_{m-1}[\theta_m]$.

One can bound the index I_m from above in terms of the discriminant Δ_{K_m} , e.g., [17] yields $I_m \leq 2^{d_m^3} \Delta_{K_m}^{(d_m-2)/4}$ (assuming K_m has no proper subfields). But for $d_m \geq 3$ this results in a trivial lower bound.

To prove Theorem 2 a more refined analysis via local heights is needed. For each rational prime p all contributions to the height above p are carefully estimated. Instead of choosing one fixed θ_m for every K_m we need to pick a suitable generator $\theta_m = \theta_m(p)$ for every prime p . Classical results on common inessential discriminant divisors, e.g., a theorem due to von Žyliński (see Theorem 3), permit us to choose $\theta_m(p)$ with the required properties, at least when p is sufficiently large in terms of d_m . Additional difficulties arise from the fact that we cannot assume $R_m = R \cap L_m$ which means we need to control the degrees d_i for $i \geq m$. The latter explains why we want the degrees d_i to be uniformly bounded.

Theorem 2 is also related to Silverman's bound [16, Theorem 2]

$$(1.13) \quad H(\alpha) \geq d_m^{-\frac{1}{d_m}} (N_{L_{m-1}/\mathbb{Q}}(\Delta_{L_m/L_{m-1}}))^{\frac{1}{2[L_{m-1}:\mathbb{Q}]d_m(d_m-1)}}.$$

The bound (1.13) applies for every $\alpha \in L_m$ with $L_{m-1}(\alpha) = L_m$. If Δ_{K_m} and $\Delta_{L_{m-1}}$ are coprime then Silverman's (1.13) recovers our (1.10) but if L_m/L_{m-1} is unramified then (1.13) gives nothing at all. To establish height lower bounds for elements in an infinite field tower $L = \bigcup_n L_n$ the inequality (1.13) is therefore only useful when the field tower is sufficiently ramified at each step. Theorem 2 allows us to get rid of this ramification condition at the expense of replacing the field L by the ring R .

A slight generalization of Northcott's Theorem shows that sets of uniformly bounded degree over any field with Northcott property also have Northcott property (see [9, Theorem 2.1]). Using this fact in conjunction with Hermite's Theorem we immediately deduce the following corollary from Theorem 2.

Corollary 1. *Suppose L_0 has the Northcott property, the family $L_0, K_1, K_2, K_3, \dots$ is linearly disjoint over $\mathbb{Q}$, and the degrees d_i are uniformly bounded from above. Moreover, suppose there is no proper intermediate field between L_{n-1} and L_n for every $n \in \mathbb{N}$. Then R also has the Northcott property.*

If the fields K_i are all cubic and $\mathbb{Q}^{(2)} \subseteq L_0$ then it suffices⁴ to assume $L_n \neq L_{n-1}$ for all but finitely many $n \in \mathbb{N}$ in place of the “linear disjointness”-condition. This proves the claim just before Definition 2, namely, that (1.6) has the Northcott property.

It is worthwhile to mention that the mere existence of a subring of $\mathcal{O}_{\mathbb{Q}^{(3)}}$ with (N) whose field of fractions is equal to $\mathbb{Q}^{(3)}$ is easy to prove. The difficulty in the proof of the above result comes from the fact that each of the components in (1.6) is a *maximal* order.

In fact, every ring contains a subring with (N) and with the same field of fractions. The proof of this statement is merely an exercise but we have not found the result in the literature and we believe it merits publication.

Proposition 1. *Let S be a subring of $\overline{\mathbb{Q}}$. Then there exists a subring T of S such that T has (N) and the field of fractions of S and of T are identical.*

We are not aware of any examples of fields K such that $\mathcal{O}_K$ has (N) but K does not (but see [11, Exemple 4.6] for a field without (N) whose ring of integers has (N) w.r.t. to a larger “height”, called house⁵).

Let us very briefly touch on two different applications of Corollary 1 and Proposition 1 for rings of totally real integers.

In 1962 Julia Robinson [15] showed that the semi-ring $(\mathbb{N}_0, 0, 1, +, \cdot)$ is first-order definable in the ring of integers of any totally real field L , provided $\mathcal{O}_L$ has (N). Vidaux and Videla [18] observed that Robinson's proof also works for arbitrary rings R of totally real integers (not necessarily the ring of integers of a field) with (N).⁶ Hence, any such ring has undecidable first-order theory.

Our next application comes from more recent work of the first author, Daans and Kala [6]. Let R be a ring of totally real integers. A totally positive definite quadratic form $Q(x_1, \dots, x_n)$ with coefficients in R is said to be universal over R if every totally positive element of R is represented by Q . Famously, the sum of four squares is universal over $\mathbb{Z}$ by Lagrange's Theorem. If R is the ring of integers a number field then there exists a universal quadratic form over R (see the survey [12] for this and more background). On the other hand, if R is *not* contained in a number field then it is usually difficult to decide whether a universal quadratic form over R exists. The answer is definitely no if R has (N), as was shown in [6, Theorem 3.2].

⁴We can replace L_0 by some L_N to assume $L_n \neq L_{n-1}$ for all n . Since $\mathbb{Q}^{(2)} \subseteq L_0$ we have L_n/L_{n-1} is Galois for every cubic K_n . Hence, $[L_n : L_{n-1}] = [K_n : \mathbb{Q}]$ for all n . Therefore the family $L_0, K_1, K_2, K_3, \dots$ is linearly disjoint over $\mathbb{Q}$, and $d_i = 3$ for all i .

⁵The house of an algebraic integer is the maximal modulus of its conjugates.

⁶In fact, it suffices if R has (N) w.r.t. the house.

Our next goal is to formulate a quantitative version of Bombieri and Zannier's Question 1. Again we will focus on the case $d = 3$. To this end we introduce the following notion of "size" for subfields of $\mathbb{Q}^{(3)}$. Since for $L \subseteq \mathbb{Q}^{(3)}$ we have "equality" if and only if L contains all cubic fields, we measure the size of a subfield L of $\mathbb{Q}^{(3)}$ by measuring how many cubic fields L contains. To this end let $N_L(X)$ be the number of cubic fields in L with modulus of the discriminant no larger than X .

Definition 3. Let L be a subfield of $\mathbb{Q}^{(3)}$. We define the size $\mathfrak{s}(L)$ of L as

$$\mathfrak{s}(L) := \liminf_{X \rightarrow \infty} \frac{\log^+ N_L(X)}{\log N_{\mathbb{Q}^{(3)}}(X)},$$

where $\log^+(x) := \log(\max\{1, x\})$.

Note that $\mathfrak{s}(L) \in [0, 1]$, $\mathfrak{s}(L_1) \leq \mathfrak{s}(L_2)$ whenever $L_1 \subset L_2$, and $\mathfrak{s}(\mathbb{Q}^{(3)}) = 1$. Here is a quantitative version of Bombieri and Zannier's question.

Question 2. How big can a subfield L of $\mathbb{Q}^{(3)}$ with Northcott property be?

Wright [22, Theorem I.2], choosing $k = \mathbb{Q}$, $G = C_3$ there, showed that the number of abelian cubic extensions grows like $X^{1/2}$. In contrast, the Davenport-Heilbronn Theorem [7] states that the total number of cubic extensions grows linearly. Thus the field $\mathbb{Q}_{ab}^{(3)}$ is a field with Northcott property and has size $1/2$.

Using a criterion of the third author [20, Corollary 4], one can easily construct larger subfields of $\mathbb{Q}^{(3)}$ with (N), say of size $\geq 3/5$ (see Section 5). But elementary constructions seem insufficient to provide a complete answer to Question 2. Fortunately, a deep result of Nakagawa provides sufficiently precise information on the distribution of cubic number fields with "nearly" prime discriminant. Combining this result with the aforementioned criterion gives the following observation which is proved in Section 5.

Proposition 2. There exists a subfield L of $\mathbb{Q}^{(3)}$ with the Northcott property and maximal size $\mathfrak{s}(L) = 1$.

2. PROOF OF PROPOSITION 1

Let $L = \text{frac}(S)$ be the field of fractions of S . If L is a number field then we can take $T = S$. Hence we can assume $L/\mathbb{Q}$ is an infinite extension. We can find a sequence of algebraic integers $(\theta_n)_n$ such that $\mathbb{Z}[\theta_1, \theta_2, \theta_3, \dots] \subseteq S$ and $L = \mathbb{Q}(\theta_1, \theta_2, \theta_3, \dots)$. Let $L_n = \mathbb{Q}(\theta_1, \dots, \theta_n)$ so that $L = \bigcup_{n \geq 1} L_n$. Furthermore, we can assume that $L_{n-1} \neq L_n$ for every $n \in \mathbb{N}$. Let us define $\alpha_1 = \theta_1$ and set $T_1 = \mathbb{Z}[\alpha_1]$. Hence, $\text{frac}(T_1) = L_1$. Now suppose we have constructed $T_{n-1} = \mathbb{Z}[\alpha_1, \dots, \alpha_{n-1}]$. Suppose T_{n-1} has field of fractions L_{n-1} . Then

$$I_{n-1} = [\mathcal{O}_{L_{n-1}} : T_{n-1}]$$

is finite and we set

$$\alpha_n = nI_{n-1}\theta_n.$$

Hence, the field of fractions of $T_n = T_{n-1}[\alpha_n]$ is equal to L_n . We set

$$T = \bigcup_{n \geq 1} T_n = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \dots].$$

Since θ_n is an algebraic integer it follows from Gauss' Lemma that its minimal polynomial

$$f_{\theta_n/L_{n-1}}(x) = x^{d_n} + a_1x^{d_n-1} + \dots + a_{d_n}$$

over L_{n-1} lies in $\mathcal{O}_{L_{n-1}}[x]$. And since $L_n \neq L_{n-1}$ it follows that $d_n > 1$. Using that $(nI_{n-1})^{d_n} f_{\theta_n/L_{n-1}}(\theta_n) = 0$ we find

$$(2.14) \quad \alpha_n^{d_n} = (nI_{n-1}\theta_n)^{d_n} = -a_1(nI_{n-1})\alpha_n^{d_n-1} - \dots - (nI_{n-1})^{d_n-1}a_{d_n-1}\alpha_n - (nI_{n-1})^{d_n}a_{d_n}.$$

Next note that

$$I_{n-1}\mathcal{O}_{L_{n-1}} \subset T_{n-1}.$$

Hence, it follows from (2.14) that

$$\alpha_n^{d_n} \in T_{n-1} + T_{n-1}\alpha_n + \dots + T_{n-1}\alpha_n^{d_n-1}.$$

Suppose $\gamma \in T$. There exists a minimal integer n such that there are polynomials $g_0, \dots, g_{d_n-1}$ in $\mathbb{Z}[x_1, \dots, x_{n-1}]$ with

$$(2.15) \quad \gamma = \sum_{i=0}^{d_n-1} g_i(\alpha_1, \dots, \alpha_{n-1})\alpha_n^i \in T_{n-1} + T_{n-1}\alpha_n + \dots + T_{n-1}\alpha_n^{d_n-1}.$$

If $g_i(\alpha_1, \dots, \alpha_{n-1}) = 0$ for $1 \leq i \leq d_n - 1$ then $\gamma = g_0(\alpha_1, \dots, \alpha_{n-1})$. This leads to an identity as in (2.15) with n replaced by $n - 1$, contradicting the minimality of n . Hence there exists $1 \leq i \leq d_n - 1$ with $g_i(\alpha_1, \dots, \alpha_{n-1}) \neq 0$.

Since $L_n = L_{n-1}(\alpha_n)$ has degree $d_n > 1$ over L_{n-1} we conclude that $L_{n-1}(\gamma) \neq L_{n-1}$. Hence, there exists a field homomorphism $\sigma : L_{n-1}(\gamma) \rightarrow \overline{\mathbb{Q}}$, not the identity, that fixes L_{n-1} . We extend σ to L_n and we write $\sigma(\beta) = \beta'$. We get

$$0 \neq \gamma - \gamma' = \sum_{i=1}^{d_n-1} g_i(\alpha_1, \dots, \alpha_{n-1})(\alpha_n^i - (\alpha'_n)^i) = (\alpha_n - \alpha'_n)G(\alpha_1, \dots, \alpha_n, \alpha'_n),$$

where $G(\alpha_1, \dots, \alpha_n, \alpha'_n)$ is some non-zero algebraic integer in the field $M = L_n(\alpha'_n)$. Set $D = [M : \mathbb{Q}]$. Using standard estimates for the height we get

$$2H(\gamma)^2 \geq H(\gamma - \gamma') \geq |N_{M/\mathbb{Q}}(\gamma - \gamma')|^{\frac{1}{D}} = |N_{M/\mathbb{Q}}(\alpha_n - \alpha'_n)|^{\frac{1}{D}} |N_{M/\mathbb{Q}}G(\alpha_1, \dots, \alpha_n, \alpha'_n)|^{\frac{1}{D}}$$

Now $\alpha_n - \alpha'_n = nI_{n-1}(\theta_n - \theta'_n)$, and $I_{n-1}(\theta_n - \theta'_n)$ and $G(\alpha_1, \dots, \alpha_n, \alpha'_n)$ are both non-zero elements in $\mathcal{O}_M$. This proves that $|N_{M/\mathbb{Q}}(\alpha_n - \alpha'_n)|^{\frac{1}{D}} \geq n$ and $|N_{M/\mathbb{Q}}G(\alpha_1, \dots, \alpha_n, \alpha'_n)|^{\frac{1}{D}} \geq 1$.

We have shown that if $\gamma \in T$ has height below $\sqrt{k/2}$ then γ lies in T_k . Since T_k is contained in the number field L_k we have only finitely many choices for γ with height below $\sqrt{k/2}$ by Northcott's Theorem. This proves that T has (N).

3. PROOF OF THEOREM 2

For the proof of Theorem 2 it is convenient to state the following nearly trivial fact as a lemma.

Lemma 1. *Let K be a subfield of $\overline{\mathbb{Q}}$, let $\theta \in \overline{\mathbb{Q}}$, and let $L = K(\theta)$. Suppose that $d = [L : K] > 1$, and let $\alpha \in L$ be such that $L = K(\alpha)$. Let $(\beta_0, \dots, \beta_{d-1}) \in K^d$ be the unique vector with $\alpha = \beta_{d-1}\theta^{d-1} + \dots + \beta_1\theta + \beta_0$. Let $\sigma_1, \dots, \sigma_d$ be the d distinct embeddings of L into $\overline{\mathbb{Q}}$, fixing K . Set*

$$s_{k,i,j} = \sum_{r=0}^k \sigma_i(\theta)^r \sigma_j(\theta)^{k-r}, \text{ and } \gamma = \prod_{1 \leq i < j \leq d} \sum_{k=0}^{d-2} \beta_{k+1} s_{k,i,j}.$$

Then

$$0 \neq \text{disc}_{L/K}(1, \alpha, \dots, \alpha^{d-1}) = \prod_{1 \leq i < j \leq d} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \text{disc}_{L/K}(1, \theta, \dots, \theta^{d-1}) \gamma^2.$$

Proof. As $L = K(\alpha)$ we conclude $0 \neq \prod_{1 \leq i < j \leq d} (\sigma_i(\alpha) - \sigma_j(\alpha))$. Further, we have

$$\sigma_i(\alpha) = \beta_{d-1}\sigma_i(\theta)^{d-1} + \dots + \beta_1\sigma_i(\theta) + \beta_0,$$

and thus

$$\sigma_i(\alpha) - \sigma_j(\alpha) = (\sigma_i(\theta) - \sigma_j(\theta)) \left(\sum_{k=0}^{d-2} \beta_{k+1} s_{k,i,j} \right).$$

Hence, we get

$$0 \neq \prod_{1 \leq i < j \leq d} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \gamma^2 \prod_{1 \leq i < j \leq d} (\sigma_i(\theta) - \sigma_j(\theta))^2 = \text{disc}_{L/K}(1, \theta, \dots, \theta^{d-1}) \gamma^2.$$

□

Lemma 2. *Let $L_0 \subseteq \overline{\mathbb{Q}}$ be a field, let $(K_i)_i$ be a sequence of number fields, and suppose*

$$\alpha \in L_m \setminus L_{m-1} \text{ and } \alpha \in R_n \setminus R_{n-1},$$

where L_m and R_n are as in (1.7). Let $\theta_m, \dots, \theta_n$ be algebraic integers with $K_i = \mathbb{Q}(\theta_i)$ for $m \leq i \leq n$, and set $I_i = [\mathcal{O}_{K_i} : \mathbb{Z}[\theta_i]]$ for $m \leq i \leq n$. Suppose that $d_i := [K_i : \mathbb{Q}] = [L_i : L_{i-1}]$ whenever $m < i \leq n$. Then there exist $\beta_{d_m-1,m-1}, \dots, \beta_{1,m-1}, \beta_{0,m-1} \in R_{m-1}$ such that

$$\alpha = \frac{1}{I_m I_{m+1} \dots I_n} \left(\beta_{d_m-1,m-1} \theta_m^{d_m-1} + \dots + \beta_{1,m-1} \theta_m + \beta_{0,m-1} \right).$$

Proof. Since $\mathcal{O}_{K_n} \subset (1/I_n)\mathbb{Z}[\theta_n]$ it follows that $R_n \subset (1/I_n)R_{n-1}[\theta_n]$. Hence, there exist

$$\beta_{d_n-1,n-1}, \beta_{d_n-2,n-1}, \dots, \beta_{0,n-1} \in R_{n-1}$$

so that

$$\alpha = \frac{1}{I_n} \left(\beta_{d_n-1,n-1} \theta_n^{d_n-1} + \dots + \beta_{1,n-1} \theta_n + \beta_{0,n-1} \right).$$

If $n > m$ then $\beta_{d_n-1,n-1} = \cdots = \beta_{1,n-1} = 0$ due to the fact that $[L_{n-1}(\theta_n) : L_{n-1}] = d_n$, and just as we did for α we can write

$$\beta_{0,n-1} = \frac{1}{I_{n-1}} \left(\beta_{d_{n-1}-1,n-2} \theta_{n-1}^{d_{n-1}-1} + \cdots + \beta_{1,n-2} \theta_{n-1} + \beta_{0,n-2} \right)$$

with $\beta_{d_{n-1}-1,n-2}, \dots, \beta_{1,n-2}, \beta_{0,n-2} \in R_{n-2}$. Continuing this way we end up with

$$\alpha = \frac{1}{I_m I_{m+1} \cdots I_n} \left(\beta_{d_m-1,m-1} \theta_m^{d_m-1} + \cdots + \beta_{1,m-1} \theta_m + \beta_{0,m-1} \right)$$

with $\beta_{d_m-1,m-1}, \dots, \beta_{1,m-1}, \beta_{0,m-1} \in R_{m-1}$. □

Next we recall the following classical result.

Theorem 3 (von Žyliński, [19]). *Let K be a number field. The field index*

$$i(K) := \gcd \{ [\mathcal{O}_K : \mathbb{Z}[\theta]] : \theta \in \mathcal{O}_K, K = \mathbb{Q}(\theta) \}$$

has the property that any rational prime p with $p \mid i(K)$ satisfies $p < [K : \mathbb{Q}]$.

Combining Lemma 1, Lemma 2, and Theorem 3 allows us to prove the following proposition.

Proposition 3. *Let $L_0 \subseteq \overline{\mathbb{Q}}$ be a field, let $(K_i)_i$ be a sequence of number fields, and suppose*

$$L_m = L_{m-1}(\alpha) \text{ and } \alpha \in R_n \setminus R_{n-1},$$

where L_m and R_n are as in (1.7). Let p be a prime, and suppose that $p \geq d_i = [L_i : L_{i-1}]$ whenever $m \leq i \leq n$. Write

$$\Delta = \text{disc}_{L_m/L_{m-1}}(1, \alpha, \dots, \alpha^{d_m-1}).$$

Then

$$\prod_{v|p} \max\{1, |\Delta^{-1}|_v\}^{\frac{d_v}{[L_m:\mathbb{Q}]}} \geq p^{\text{ord}_p(\Delta_{K_m})}.$$

Proof. We apply Lemma 2 to get

$$\alpha = \frac{1}{I_m I_{m+1} \cdots I_n} \left(\beta_{d_m-1,m-1} \theta_m^{d_m-1} + \cdots + \beta_{1,m-1} \theta_m + \beta_{0,m-1} \right).$$

Since $p \geq d_i$ whenever $m \leq i \leq n$ it follows from von Žyliński's Theorem 3 that we can choose the integral generators $\theta_m, \dots, \theta_n$ such that with $I = I_m I_{m+1} \cdots I_n$

$$p \nmid I.$$

Next we apply Lemma 1 with $K = L_{m-1}$, $L = L_m$, $d = d_m > 1$ (note that $L = K(\alpha)$) and

$$\beta_i = \frac{\beta_{i,m-1}}{I}$$

for all $0 \leq i \leq d_m - 1$ to get

$$0 \neq \Delta = \text{disc}_{L_m/L_{m-1}}(1, \theta_m, \dots, \theta_m^{d_m-1}) \gamma^2,$$

where

$$\gamma^2 = \frac{B^2}{I^{d_m(d_m-1)}},$$

and B is a non-zero algebraic integer.

Since $d_m = [L_m : L_{m-1}]$ and $K_m = \mathbb{Q}(\theta_m)$ we infer

$$\text{disc}_{L_m/L_{m-1}}(1, \theta_m, \dots, \theta_m^{d_m-1}) = \text{disc}_{K_m/\mathbb{Q}}(1, \theta_m, \dots, \theta_m^{d_m-1}) = \Delta_{\mathbb{Z}[\theta_m]},$$

so that we conclude

$$\Delta = \Delta_{\mathbb{Z}[\theta_m]} \cdot \frac{B^2}{I^{d_m(d_m-1)}}.$$

If $p \nmid \Delta_{K_m}$, then the statement follows at once. If $p \mid \Delta_{K_m}$, then

$$\prod_{v|p} \max\{1, |\Delta^{-1}|_v\}^{\frac{d_v}{[L_m:\mathbb{Q}]}} \geq \prod_{v|p} |\Delta^{-1}|_v^{\frac{d_v}{[L_m:\mathbb{Q}]}} = \prod_{v|p} \left| \frac{I^{d_m(d_m-1)}}{\Delta_{\mathbb{Z}[\theta_m]} B^2} \right|_v^{\frac{d_v}{[L_m:\mathbb{Q}]}} \geq \left| \frac{I^{d_m(d_m-1)}}{\Delta_{\mathbb{Z}[\theta_m]}} \right|_p \geq p^{\text{ord}_p(\Delta_{K_m})},$$

as $\Delta_{K_m} \mid \Delta_{\mathbb{Z}[\theta_m]}$, and $p \nmid I$. □

We are now ready to prove Theorem 2.

Proof of Theorem 2. Let $\alpha \in R$ and $L_{m-1}(\alpha) = L_m$. Recall that $\Delta = \text{disc}_{L_m/L_{m-1}}(1, \alpha, \dots, \alpha^{d_m-1})$. Using the basic inequalities $H(a+b) \leq 2H(a)H(b)$, $H(ab) \leq H(a)H(b)$, and the fact that conjugates have equal height, we conclude

$$(3.16) \quad H(\Delta) = H \left(\prod_{1 \leq i < j \leq d_m} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \right) \leq (\sqrt{2}H(\alpha))^{2d_m(d_m-1)}.$$

Next we note that $H(\Delta) = H(\Delta^{-1})$. By hypothesis of the theorem and Remark 1 we have $d_i = [K_i : \mathbb{Q}] = [L_i : L_{i-1}]$ for every $i \in \mathbb{N}$. Since $\alpha \notin L_{m-1}$ there exists $n \geq m$ such that $\alpha \in R_n \setminus R_{n-1}$. Using Proposition 3 we get

$$H(\Delta) = H(\Delta^{-1}) \geq \prod_{p \geq d} \prod_{v|p} \max\{1, |\Delta^{-1}|_v\}^{\frac{d_v}{[L_m:\mathbb{Q}]}} \geq \prod_{p \geq d} p^{\text{ord}_p(\Delta_{K_m})} = \frac{|\Delta_{K_m}|}{\prod_{p < d} p^{\text{ord}_p(\Delta_{K_m})}}.$$

But we have $\text{ord}_p(\Delta_{K_m}) \leq C_d$ (see [4, Theorem B.2.12], and using that $d_m \leq d$), and therefore we get

$$H(\Delta) \geq d^{-dC_d} |\Delta_{K_m}|.$$

Combining the latter with (3.16) proves the claim. $\square$

4. A VARIATION OF THEOREM 1

It would be desirable to replace the hypothesis that the degrees d_i be prime in Theorem 1 by the weaker hypothesis that L_i/L_{i-1} has no proper intermediate field. This can be done if we assume that the family of Galois closures of $L_0, K_1, K_2, K_3, \dots$ is linearly disjoint over $\mathbb{Q}$.

Theorem 4. *Let $L_0, (K_n)_n, (L_n)_n$ be as in Definition 2 (b), and suppose the Galois closures of $L_0, K_1, K_2, K_3, \dots$ are linearly disjoint over $\mathbb{Q}$. Moreover, suppose there is no proper intermediate field between L_{n-1} and L_n for every $n \in \mathbb{N}$, and all degrees d_n are bounded from above by some $d \in \mathbb{N}$. Then there exists $c_d > 0$, depending only on d , such that for every $\alpha \in R$*

$$H(\alpha) \geq c_d (\log[L_0(\alpha) : L_0])^{\frac{1}{d^3}}.$$

The proof is almost the same as for Theorem 1 starting by reordering the fields K_i by increasing discriminant $|\Delta_{K_i}|$ and thus redefining the sequence of fields L_i . Assuming the new family of fields L_i still satisfies the “no intermediate fields” condition we can proceed exactly as for the proof of Theorem 1 in the Introduction. The following lemma provides the missing piece.

Lemma 3. *Let $L_0, (K_n)_n$, and $(L_n)_n$ be as in Definition 2 (b), and suppose the Galois closures of $L_0, K_1, K_2, K_3, \dots$ are linearly disjoint over $\mathbb{Q}$. Write $K'_n = K_{\sigma(n)}$ for $n \in \mathbb{N}$, and $L'_n = L_0 \prod_{i=1}^n K'_i$. Then there exists a proper intermediate field between L_n and L_{n-1} for some $n \in \mathbb{N}$ if and only if there exists a proper intermediate field between L'_m and L'_{m-1} for some $m \in \mathbb{N}$.*

Proof. First we consider the following special case, where $\sigma = \tau_{(1,2)}$ is the transposition (1, 2).

- (1) (Going up) Suppose M is a proper intermediate field between L_0 and L_1 . We claim that MK_2 is a proper intermediate field between L'_1 and L'_2 . Clearly $L'_1 \subseteq MK_2 \subseteq L'_2$, so it remains to argue that MK_2 cannot be L'_1 or L'_2 . If $MK_2 = L'_1 = L_0K_2$, then we have $L_0 \subsetneq M \subseteq L_1 \cap L'_1 = L_1 \cap MK_2$, which contradicts the linear disjointness of L_0, K_1, K_2 . If $MK_2 = L'_2 = L_2$, then we have $L_1 \subsetneq MK_2$. But then linear disjointness forces $M = L_1$. So the claim holds.
- (2) (Going down) Suppose M is a proper intermediate field between L_1 and L_2 . We write $\widetilde{K}_2$ for the Galois closure of K_2 , and H for the subgroup of $G = \text{Gal}(\widetilde{K}_2 L_1 / L_1)$ whose fixed field is L_2 . Hence there is a subgroup $H \subsetneq H_M \subsetneq G$ whose fixed field is M . The hypothesis implies that $L_0, \widetilde{K}_2$ and K_1 are linearly disjoint over $\mathbb{Q}$, and so $[\widetilde{K}_2 L_1 : L_1] = [\widetilde{K}_2 L_0 : L_0]$. Hence, the injective group homomorphism

$$\phi : \text{Gal}(\widetilde{K}_2 L_1 / L_1) \rightarrow \text{Gal}(\widetilde{K}_2 L_0 / L_0),$$

sending σ to its restriction $\sigma|_{\widetilde{K}_2 L_0}$, defines an isomorphism. The fixed fields of $\phi(H)$ and $\phi(G)$ are L'_1 and L_0 respectively. Hence, the fixed field of $\phi(H_M)$ is a proper intermediate field between L_0 and L'_1 .

Applying the arguments above with L_{n-1}, K_n, K_{n+1} in place of L_0, K_1, K_2 respectively, we find that the existence of a proper intermediate field in the chain $L_0 \subseteq L_1 \subseteq \dots$ is preserved under transposition $\tau_{(n,n+1)}$. Furthermore, the claims above actually show that for an arbitrary transposition τ , if there is a proper intermediate field between L_m and L_{m-1} for some $m \in \mathbb{N}$, then there is a proper intermediate field between $L'_{\tau(m)}$ and $L'_{\tau(m)-1}$.

Finally, let $\sigma : \mathbb{N} \rightarrow \mathbb{N}$ be an arbitrary bijective function, and suppose there exists a proper intermediate field between L_n and L_{n-1} for some $n \in \mathbb{N}$. Then there exists a bijective function $\rho : \mathbb{N} \rightarrow \mathbb{N}$ that is the composition of finitely many transpositions, such that $\rho^{-1}(m) = \sigma^{-1}(m)$ for every $m \leq \sigma(n)$. Writing $K''_n = K_{\rho(n)}$ for $n \in \mathbb{N}$ and $L''_n = L_0 \prod_{i=1}^n K''_i$, we have $L'_m = L''_m$ for every $m \leq \sigma(n)$, and the claim implies that there is a proper intermediate field between $L''_{\sigma(n)} = L'_{\sigma(n)}$ and $L''_{\sigma(n)-1} = L'_{\sigma(n)-1}$. $\square$

5. PROOF OF PROPOSITION 2

The proof of Proposition 2 uses a result of Nakagawa and a general criterion for the Northcott property [20, Theorem 3]. For our purposes the following special case is most convenient.

Corollary 2 (Widmer, [20, Corollary 4]). *Let K_0 be a number field. Let $K_1, K_2, \dots$ be a sequence of field extensions of K_0 such that $[K_i : K_0] \leq 3$. Suppose for every i there exists a prime p_i so that $p_i \mid \Delta_{K_i}$ and $p_i \nmid \Delta_{K_j}$ for $0 \leq j < i$. Then,*

$$K_0 \prod_{n \geq 1} K_n$$

has (N).

Before proving Proposition 2 let us give a simple construction of a subfield of $\mathbb{Q}^{(3)}$ with (N) and size $\geq 3/5$. To this end let $p > 2$ be a prime and consider $D_p(x) = x^3 + Ax + B$. We make the ansatz $A = -3n^2$ and $B = 2n^3 + 2p$ and then choose n to be the even integer closest to $-(p/2)^{1/3}$. Thus, D_p is irreducible over $\mathbb{Q}$ and its discriminant

$$-4A^3 - 27B^2 = -108p(2n^3 + p)$$

is divisible by p and of size $O(p^{5/3})$. In particular, p^2 does not divide the discriminant of D_p once $p > 3$ because $108 = 2^2 3^3$. Moreover, if $q < p$ are both primes, then p cannot divide the discriminant of D_q since otherwise it would be at least $qp > q^2$. Setting $K_p = \mathbb{Q}(\alpha_p)$, where α_p is any root of D_p , we conclude that p ramifies in K_p but not in K_q (for q smaller than p) and $|\Delta_{K_p}| = O(p^{5/3})$. By Corollary 2, the composite field of all these cubic fields K_p (one for each prime p) yields a Property (N) field L with $\mathfrak{s}(L) \geq 3/5$.

Now let us prove Proposition 2. First we show that for every odd prime p , there exists a cubic number field F_p such that $p \mid \Delta_{F_p}$ and $|\Delta_{F_p}| \leq 324p$. For $p = 3$, let $F_3 = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - 3x - 1$. Then $\Delta_{F_3} = 81$. Assume now $p \neq 3$. We appeal to the following result.

Theorem 5 (Nakagawa, [13, Theorem 0.4]). *Let $-n$ be a discriminant of an imaginary quadratic field, $3 \nmid n$. Then*

$$\mathfrak{N}(-n) + \mathfrak{N}(-81n) = 3\mathfrak{N}(3n) + 1,$$

where $\mathfrak{N}(d)$ denotes the number of cubic number fields with discriminant d .

In the theorem above, the right-hand side equals $3\mathfrak{N}(3n) + 1 \geq 1$, implying that either $\mathfrak{N}(-n) \geq 1$ or $\mathfrak{N}(-81n) \geq 1$, i.e., there exists a cubic number field with discriminant $-n$ or $-81n$. Taking an odd prime p , depending on whether $p \equiv 1$ or $3 \pmod{4}$, we let $n = 4p$ or p , respectively. These choices ensure, by Nakagawa's theorem, that there exists a cubic field F_p with $\Delta_{F_p} \in \{-p, -4p, -81p, -324p\}$, so that $p \mid \Delta_{F_p}$ and $|\Delta_{F_p}| \leq 324p$, where $324 = 2^2 3^4$.

Finally, each Δ_{F_p} is divisible only by 2, 3 and p , so $p \nmid \Delta_{F_q}$ for $q < p$ as soon as $p > 3$. Hence we apply Corollary 2 to $K_0 = \mathbb{Q}$ and $K_i = F_{p_i}$. The compositum of all these fields L has Property (N). L contains a cubic field of discriminant at most X for every prime $p \leq X/324$, hence $N_L(X) \gg X \log X$ and $\mathfrak{s}(L) = 1$, as was required to show.

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**, no.2 (2000), 260–272.
3. F. Amoroso and D. W. Masser, *Lower bounds for the height in Galois extensions*, Bull. Lond. Math. Soc. **48**, no.6 (2016), 1008–1012.
4. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
5. E. Bombieri and U. Zannier, *A Note on heights in certain infinite extensions of $\mathbb{Q}$* , Rend. Mat. Acc. Lincei **12** (2001), 5–14.
6. N. Daans, V. Kala, and S. H. Man, *Universal quadratic forms and Northcott property of infinite number fields*, J. Lond. Math. Soc. (2) **110** (2024), no. 5, Paper No. e70022, 20. MR 4822246
7. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic field extensions. II*, Proc. London. Math. Soc. **322** (1971), 405–420.
8. A. B. Dixit and S. Kala, *On points of small height in infinite extensions*, ANNALI SCUOLA NORMALE SUPERIORE - CLASSE DI SCIENZE, **31**, 2026.
9. R. Dvornicich and U. Zannier, *On the properties of Northcott and Narkiewicz for fields of algebraic numbers*, Functiones et Approximatio **39** (2008), 163–173.
10. M. D. Fried and M. Jarden, *Field Arithmetic*, Springer, 2005.
11. E. Gaudron and G. Rémond, *Corps de Siegel*, J. reine angew. Math. **726** (2017), 187–247.
12. V. Kala, *Universal quadratic forms and indecomposables in number fields: a survey*, Commun. Math. **31** (2023), no. 2, 81–114. MR 4621253
13. J. Nakagawa, *On the relations among the class numbers of binary cubic forms*, Invent. Math. **134** (1998), no. 1, 101–138.
14. D. G. Northcott, *Periodic points on an algebraic variety*, Ann. of Math. **51** (1950), 167–177.
15. J. Robinson, *On the decision problem for algebraic rings*, Studies in mathematical analysis and related topics, Stanford Univ. Press, Stanford (1962), 297–304.
16. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
17. J. L. Thunder, *An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma*, J. reine angew. Math. **475** (1996), 167–185.
18. X. Vidaux and C. R. Videla, *Definability of the natural numbers in totally real towers of nested square roots*, Proc. Amer. Math. Soc. **143**, no.10 (2015), 4463–4477.

19. E. von Žyliński, *Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Körper.*, Math. Ann. **73.2** (1913), 273–274.
20. M. Widmer, *On certain infinite extensions of the rationals with Northcott property*, Monatsh. Math. **162** (2011), no. 3, 341–353.
21. M. Widmer, *On the Northcott property for infinite extensions*, Essent. Number Theory **2** (2023), no. 1, 1–14. MR 4681466
22. D. J. Wright, *Distribution of discriminants of abelian extensions*, Proceedings of the London Mathematical Society **3** (1989), no. 1, 17–50.

(S.H.M., P.Y.) CHARLES UNIVERSITY, FACULTY OF MATHEMATICS AND PHYSICS, DEPARTMENT OF ALGEBRA, SOKOLOVSKÁ 83, 186 75 PRAHA 8, CZECH REPUBLIC

(N.T.) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN–MADISON, 480 LINCOLN DRIVE, MADISON, WI 53706, USA

(M.W.) GRAZ UNIVERSITY OF TECHNOLOGY, INSTITUTE OF ANALYSIS AND NUMBER THEORY, STEYRERGASSE 30/II, 8010 GRAZ, AUSTRIA

Email address, S. H. Man: `shman@karlin.mff.cuni.cz`

Email address, N. Technau: `technau@wisc.edu`

Email address, M. Widmer: `martin.widmer@tugraz.at`

Email address, P. Yatsyna: `p.yatsyna@mff.cuni.cz`