Noname manuscript No.
(will be inserted by the editor)

On certain infinite extensions of the rationals with Northcott property

Martin Widmer

Received: date / Accepted: date

Abstract A set of algebraic numbers has the Northcott property if each of its subsets of bounded Weil height is finite. Northcott's Theorem, which has many Diophantine applications, states that sets of bounded degree have the Northcott property. Bombieri, Dvornicich and Zannier raised the problem of finding fields of infinite degree with this property. Bombieri and Zannier have shown that $\mathbb{Q}_{ab}^{(d)}$, the maximal abelian subfield of the field generated by all algebraic numbers of degree at most d, is such a field. In this note we give a simple criterion for the Northcott property and, as an application, we deduce several new examples, e.g. $\mathbb{Q}(2^{1/d_1}, 3^{1/d_2}, 5^{1/d_3}, 7^{1/d_4}, 11^{1/d_5}, ...)$ has the Northcott property if and only if $2^{1/d_1}, 3^{1/d_2}, 5^{1/d_3}, 7^{1/d_4}, 11^{1/d_5}, ...$ tends to infinity.

Keywords Northcott property · height · preperiodic points · field arithmetic

Mathematics Subject Classification (2000) 12F05 · 11G50

1 Introduction

Let $\mathcal{A}$ be a subset of the algebraic numbers $\overline{\mathbb{Q}}$ and denote by $H(\cdot)$ the non-logarithmic absolute Weil height on $\overline{\mathbb{Q}}$ as defined in [1]. Following Bombieri and Zannier [2] we say $\mathcal{A}$ has the Northcott property, short property (N), if for each positive real number X there are only finitely many elements α in $\mathcal{A}$ with $H(\alpha) \leq X$. The 1-dimensional version of Northcott's Theorem (see [15] Theorem 1) states that sets of algebraic numbers with uniformly bounded degree (over $\mathbb{Q}$) have property (N). Northcott's Theorem has

This work has been financially supported by the Swiss National Science Foundation.

M. Widmer
Department of Mathematics, University of Texas at Austin,
1 University Station C1200, Austin, TX 78712, USA
E-mail: Widmer@math.utexas.edu
Present address:
Institut für Mathematik A, Technische Universität Graz,
Steyrergasse 30/II, 8010 Graz, Austria
Tel.: +43-316-8737620
Fax: +43-316-8737126
E-mail: Widmer@tugraz.at

been used extensively, especially to deduce finiteness results in Diophantine geometry. Other applications will be mentioned briefly in Section 11. Bombieri and Zannier [2] and more explicitly Dvornicich and Zannier ([4] p.165) proposed the problem of finding other fields than number fields with property (N). In this note we give a simple sufficient criterion for an infinite extension of $\mathbb{Q}$ to have property (N). Our criterion depends on the growth rate of certain discriminants. The method uses a lower bound due to Silverman for the height of an element generating the number field. As an application we deduce property (N) for several infinite extensions, here is just one example; with positive integers d_i the extension $\mathbb{Q}(2^{1/d_1}, 3^{1/d_2}, 5^{1/d_3}, 7^{1/d_4}, 11^{1/d_5}, ...)$ has property (N) if and only if $2^{1/d_1}, 3^{1/d_2}, 5^{1/d_3}, 7^{1/d_4}, 11^{1/d_5}, ...$ tends to infinity.

For an arbitrary number field K and a positive integer d let $K^{(d)}$ be the compositum of all field extensions of K of degree at most d. Bombieri and Zannier [2] addressed the following question: *does $K^{(d)}$ have property (N)?* So far the only contribution to this question is due to Bombieri and Zannier ([2] Theorem 1.1). Let us write $K_{ab}^{(d)}$ for the compositum of all abelian extensions F/K with $K \subseteq F \subseteq K^{(d)}$.

Theorem 1 (Bombieri, Zannier) *The field $K_{ab}^{(d)}$ has property (N), for any positive integer d.*

Since $K^{(2)} = K_{ab}^{(2)}$ Theorem 1 positively answers Bombieri and Zannier's question for $d = 2$. However, for $d > 2$ the question whether $K^{(d)}$ has property (N) remains open. Another consequence of Theorem 1 is the following result.

Corollary 1 (Bombieri, Zannier) *For any positive integer d the field $\mathbb{Q}(1^{1/d}, 2^{1/d}, 3^{1/d}, 4^{1/d}, 5^{1/d}, ...)$ has property (N).*

Dvornicich and Zannier ([4] Theorem 2.1) observed that by a small variation of Northcott's argument the ground field $\mathbb{Q}$ in Northcott's Theorem can be replaced by any field with property (N). This turns out to be a very useful fact so that we state it explicitly as a theorem.

Theorem 2 *Let L be a field of algebraic numbers with property (N) and let $d > 0$ be an integer. The set of algebraic numbers of degree at most d over L has property (N). In particular every finite extension of L has the property (N).*

Taking a finite extension of a field with property (N) is of course a very special case of taking the compositum of two fields with property (N). So one might ask: is the property (N) preserved under taking the compositum of two fields? We shall see that this is not always the case.

Before we state our own results let us fix some basic notation. All fields are considered to lie in a fixed algebraic closure of $\mathbb{Q}$. For positive rational integers a, b the expression $a^{1/b}$ denotes the real positive b-th root of a, unless stated otherwise. By a prime ideal we always mean a non-zero prime ideal. Let F, M, K be number fields with $F \subseteq M \subseteq K$ and write $\mathcal{O}_K$ for the ring of integers in K. For a non-zero fractional ideal $\mathfrak{A}$ of $\mathcal{O}_K$ in K let $D_{K/M}(\mathfrak{A})$ be the discriminant-ideal of $\mathfrak{A}$ relative to M (for the definition see [8] p.65) and write $D_{K/M}$ for $D_{K/M}(\mathcal{O}_K)$ (see also [14] p.201). Let us denote by $N_{M/F}(\cdot)$ the norm from M to F as defined in [8] p.24. Then we have

$$D_{K/F} = D_{M/F}^{[K:M]} N_{M/F}(D_{K/M}) \tag{1}$$

(see [14] (2.10) Corollary p.202). For a non-zero fractional ideal $\mathfrak{B}$ of $\mathcal{O}_M$ in M we interpret the principal ideal $N_{M/\mathbb{Q}}(\mathfrak{B})$ as the unique positive rational generator of this ideal. Note that $D_{K/M}$ is an integral ideal in $\mathcal{O}_M$ and thus $N_{M/\mathbb{Q}}(D_{K/M})$ is in $\mathbb{Z}$. We write Δ_K for the absolute discriminant of K so that $D_{K/\mathbb{Q}}$ is the principal ideal generated by Δ_K. In particular (1) yields

$$|\Delta_K| = |\Delta_M|^{[K:M]} N_{M/\mathbb{Q}}(D_{K/M}). \tag{2}$$

We will also frequently use the following fact (see [6] Theorem 85 p.97): let F, K be two number fields. A prime p in $\mathbb{Z}$ ramifies in the compositum of F and K if and only if it ramifies in F or in K.

So far Theorem 1, and its immediate consequences, were the only sources for fields of infinite degree with property (N). Our first result is a simple but rather general criterion for the property (N) concerning subfields of $\overline{\mathbb{Q}}$. Roughly speaking it states that the union of fields in a saturated (i.e. without intermediate fields) nested sequence of number fields with enough ramification at each step has property (N).

Theorem 3 *Let K be a number field, let $K = K_0 \subsetneq K_1 \subsetneq K_3 \subsetneq ....$ be a nested sequence of finite extensions and set $L = \bigcup_i K_i$. Suppose that*

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \left(N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}) \right)^{\frac{1}{[M:K_0][M:K_{i-1}]}} \longrightarrow \infty \tag{3}$$

as i tends to infinity where the infimum is taken over all intermediate fields M strictly larger than K_{i-1}. Then the field L has the Northcott property.

If the nested sequence of number fields is saturated then (3) simplifies to

$$N_{K_{i-1}/\mathbb{Q}}(D_{K_i/K_{i-1}})^{\frac{1}{[K_i:K_0][K_i:K_{i-1}]}} \longrightarrow \infty. \tag{4}$$

In the sequel we give several applications of Theorem 3. For a number field K and a prime ideal $\wp$ of $\mathcal{O}_K$ we say $D = x^d + a_1 x^{d-1} + ... + a_d$ in $\mathcal{O}_K[x]$ is a $\wp$-Eisenstein polynomial if $a_j \in \wp$ for $1 \leq j \leq d$ and $a_d \notin \wp^2$. Such a polynomial is irreducible over K (see [10] p.256). As a consequence of Theorem 3 we deduce the following theorem.

Theorem 4 *Let K be a number field, let $p_1, p_2, p_3, ...$ be a sequence of positive prime numbers and for $i = 1, 2, 3, ...$ let D_i be a p_i-Eisenstein polynomial in $\mathbb{Z}[x]$. Denote $\deg D_i = d_i$ and let α_i be any root of D_i. Moreover suppose that $p_i \nmid \Delta_{\mathbb{Q}(\alpha_j)}$ for $1 \leq j < i$ and that $p_i^{1/d_i} \longrightarrow \infty$ as i tends to infinity. Then the field $K(\alpha_1, \alpha_1, \alpha_3, ...)$ has the Northcott property.*

Theorem 4 implies a refinement of Corollary 1. This refinement shows that the condition $p_i^{1/d_i} \longrightarrow \infty$ in Theorem 4 cannot be weakened.

Corollary 2 *Let K be a number field, let $p_1 < p_2 < p_3 < ...$ be a sequence of positive primes and let $d_1, d_2, d_3, ...$ be a sequence of positive integers. Then the field $K(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, ...)$ has the Northcott property if and only if $|p_i^{1/d_i}| \longrightarrow \infty$ as i tends to infinity. Here p_i^{1/d_i} is any d_i-th root of p_i and $|\cdot|$ denotes the complex modulus.*

If the d_i are prime and not uniformly bounded then $\mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, ...)$ contains elements of arbitrarily large prime degree and thus it cannot be generated over $\mathbb{Q}$ by algebraic numbers of bounded degree. The conclusion remains true if we drop the primality condition on d_i. This can be deduced from Proposition 1 in [2] which implies for any subfield $L \subseteq \mathbb{Q}^{(d)}$ the local degrees $[L_v : \mathbb{Q}_v]$ are bounded solely in terms of d. Now the local degrees of $L = \mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, ...)$ are not uniformly bounded and so L is not contained in $\mathbb{Q}^{(d)}$ for any choice of d. To the best of the author's knowledge Corollary 2 provides the first such example of a field with property (N). Moreover, Corollary 2 easily implies the following statement.

Theorem 5 *Property (N) is not generally preserved under taking the composite of two fields. More concretely: let p_i be the $i+1$-th prime number and set $d_i = [\sqrt{\log p_i}]$. Let*

$$L_1 = \mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, ...),$$
$$L_2 = \mathbb{Q}(p_1^{1/(d_1+1)}, p_2^{1/(d_2+1)}, p_3^{1/(d_3+1)}, ...).$$

Then L_1 and L_2 both have property (N) but their composite field does not have property (N).

Another example proving Theorem 5, again coming from Corollary 2, is as follows: consider the fields $L_1 = \mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, ...)$ and $L_2 = \mathbb{Q}(\zeta_1 p_1^{1/d_1}, \zeta_2 p_2^{1/d_2}, \zeta_3 p_3^{1/d_3}, ...)$, where d_i is as in Theorem 5 and ζ_i are primitive d_i-th roots of unity. Then plainly L_1, L_2 have the property (N) (by Corollary 2) but $L_1 L_2$ does not because it contains infinitely many roots of unity.

Let us give one more immediate consequence of Theorem 4. This result can be considered as a very small step towards the validity of property (N) for $K^{(d)}$.

Corollary 3 *Let d be a positive integer, let F_0 be an arbitrary number field and let $F_1, F_2, F_3, ...$ be a sequence of finite extensions of F_0 with $[F_i : F_0] \leq d$. Moreover suppose there exists a sequence $p_1, p_2, p_3, ...$ of positive prime numbers such that p_i ramifies totally in F_i but does not ramify in F_j for $1 \leq j < i$. Then the compositum of $F_0, F_1, F_2, F_3, ...$ has the Northcott property.*

In the case $d = 3$ one can apply the criterion from Theorem 3 directly to prove a stronger result.

Corollary 4 *Let F_0 be an arbitrary number field and let $F_1, F_2, F_3, ...$ be a sequence of field extensions of F_0 with $[F_i : F_0] \leq 3$ such that for each positive integer i there is a prime p_i with $p_i \mid \Delta_{F_i}$ and $p_i \nmid \Delta_{F_j}$ for $0 \leq j < i$. Then the compositum of $F_0, F_1, F_2, F_3, ...$ has the Northcott property.*

As a next step towards $K^{(3)}$ we would like to replace F_i in Corollary 4 by its Galois closure $F_i^{(g)}$ over F_0. Unfortunately we have to impose an additional technical condition and we also restrict F_0 to $\mathbb{Q}$.

Corollary 5 *Let $F_1, F_2, F_3, ...$ be a sequence of field extensions with $[F_i : \mathbb{Q}] \leq 3$ such that for each integer $i > 1$ there is a prime p_i with $p_i \mid \Delta_{F_i}$ and $p_i \nmid \Delta_{F_j}$ for $1 \leq j < i$. Furthermore suppose that for each $i > 1$ at least one of the following conditions holds:*
(a)$F_i/\mathbb{Q}$ is Galois.
(b)$F_i = \mathbb{Q}(\alpha)$ for an α with $\alpha^3 \in \mathbb{Q}$.

(c)$F_i = \mathbb{Q}(\alpha)$ *for an algebraic integer* α *with* $2 \nmid \mathrm{ord}_{p_i}\, Disc(D_\alpha)$ *for the monic minimal polynomial* $D_\alpha \in \mathbb{Z}[x]$ *of* α.
(d)$F_i = \mathbb{Q}(\alpha)$ *for a root* α *of a polynomial of the form* $x^3 + a_0 c^3 x^l + b_0^l c^3$ *with* $l \in \{1, 2\}$ *and rational integers* a_0, b_0, c *satisfying* $\gcd(2a_0c, 3b_0) = 1$.
Then the compositum of $F_1^{(g)}, F_2^{(g)}, F_3^{(g)}, ...$ *has the Northcott property.*

Theorem 4, Corollary 3, Corollary 4, and Corollary 5 can be generalized in various ways, for instance the constraints in these results can be relaxed by computing the contribution to the relative discriminant of more than just one prime.

2 A simple observation

Let L be a field of algebraic numbers of infinite degree. Now we consider a nested sequence of fields

$$K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq ...$$

such that

$$\begin{aligned}&(i)\ \ K_0 \text{ has the property } (N),\\ &(ii)\ [K_i : K_{i-1}] < \infty \text{ for } i > 0,\\ &(iii) L = \bigcup_{i=0}^{\infty} K_i.\end{aligned}$$

For a finite extension M/F of subfields of $\overline{\mathbb{Q}}$ we define

$$\delta(M/F) = \inf\{H(\alpha); F(\alpha) = M\}.$$

Note that if M has the property (N) then the infimum is attained, i.e. there exists $\alpha \in M$ with $F(\alpha) = M$ and $H(\alpha) = \delta(M/F)$.
Since each K_i is a finite extension of K_0 we deduce by (i) and Theorem 2 that each field K_i has property (N).

Proposition 1 *L has property (N) if and only if*

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}) \longrightarrow \infty \qquad \textit{as } i \to \infty$$

where the infimum is taken over all intermediate fields M strictly larger than K_{i-1}.

Although it is not needed here, we point out that for $i > 0$

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}) = \inf_{\alpha \in K_i \backslash K_{i-1}} H(\alpha)$$

and this holds even if K_i does not have property (N). The inequality "$\leq$" is obvious. For "$\geq$" let M be a field with $K_{i-1} \subsetneq M \subseteq K_i$ and let $\alpha_1, \alpha_2, \alpha_3, ...$ be a sequence in M with $K_{i-1}(\alpha_j) = M$ and $H(\alpha_j) \to \delta(M/K_{i-1})$ as $j \to \infty$. Then clearly $\alpha_j \in K_i \backslash K_{i-1}$ and thus $H(\alpha_j) \geq \inf_{\alpha \in K_i \backslash K_{i-1}} H(\alpha)$. This shows that $\delta(M/K_{i-1}) \geq \inf_{\alpha \in K_i \backslash K_{i-1}} H(\alpha)$ which proves the inequality "$\geq$".

Proof (of Proposition 1) For brevity let us write

$$A_i = \inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}).$$

First we show that property (N) for the field L implies $A_i \to \infty$.
For each $i > 0$ we can find $\alpha_i \in K_i \backslash K_{i-1}$ with $H(\alpha_i) = A_i$, in particular the elements α_i are pairwise distinct. Now suppose $(A_i)_{i=1}^{\infty}$ has a bounded subsequence. Hence we get infinitely many elements $\alpha_i \in L$ with uniformly bounded height and so L does not have property (N).

Next we prove that $A_i \to \infty$ implies property (N) for the field L.
Suppose L does not have property (N). Hence there exists an infinite sequence $\alpha_1, \alpha_2, \alpha_3, ...$ of pairwise distinct elements in $L \backslash K_0$ with $H(\alpha_j) \leq X$ for a certain fixed real number X. Let $i = i(\alpha_j)$ be such that $\alpha_j \in K_i \backslash K_{i-1}$. Thus

$$K_{i-1} \subsetneq K_{i-1}(\alpha_j) \subseteq K_i$$

and hence

$$A_i \leq \delta(K_{i-1}(\alpha_j)/K_{i-1}) \leq H(\alpha_j) \leq X.$$

Since each field K_i has the property (N) we conclude $i(\alpha_j) \longrightarrow \infty$ as $j \to \infty$. Thus $(A_i)_{i=1}^{\infty}$ has a bounded subsequence.

3 Silverman's inequality

In order to apply Proposition 1 we need a lower bound for the invariant $\delta(M/K)$. A good lower bound was proven by Silverman if both fields are number fields. So let K, M be number fields with $K \subseteq M$ and $m = [M : K] > 1$. Let α be a primitive point of the extension M/K, i.e. $M = K(\alpha)$. We apply Silverman's Theorem 2 from [18] with $F = K$ and $K = M$ and with Silverman's S_F as the set of archimedean absolute values. Then Silverman's $L_F(\cdot)$ is simply the usual norm $N_{F/\mathbb{Q}}(\cdot)$ and we deduce

$$H(\alpha)^{[K:\mathbb{Q}]} \geq \exp\left(-\frac{\delta_K \log m}{2(m-1)}\right) N_{K/\mathbb{Q}}(D_{M/K})^{\frac{1}{2m(m-1)}} \tag{5}$$

where δ_K is the number of archimedean places of K. Since Silverman used an "absolute height relative to K" rather than an absolute height, we had to take the $[K : \mathbb{Q}]$-th power on the left hand side of (5).

4 Proof of Theorem 3

From Proposition 1 we know it suffices to show

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}) \longrightarrow \infty \qquad \text{as } i \to \infty.$$

So let M be an intermediate field $K_{i-1} \subsetneq M \subseteq K_i$ and set $m = [M : K_{i-1}]$. We apply (5) with K replaced by K_{i-1}. Then taking the $[K_{i-1} : \mathbb{Q}]$-th root and using $\delta_{K_{i-1}} \leq [K_{i-1} : \mathbb{Q}]$ we conclude for any $\alpha \in M$ with $K_{i-1}(\alpha) = M$

$$H(\alpha) \geq m^{-\frac{1}{2(m-1)}} (N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}))^{\frac{1}{2[K_{i-1}:\mathbb{Q}]m(m-1)}}.$$

In particular

$$\inf_{K_{i-1} \subsetneq M \subseteq K_i} \delta(M/K_{i-1}) \geq (1/2) \inf_{K_{i-1} \subsetneq M \subseteq K_i} (N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}))^{\frac{1}{2[K_{i-1}:\mathbb{Q}]m(m-1)}}. \tag{6}$$

Now using $[K_{i-1} : \mathbb{Q}]m = [K_0 : \mathbb{Q}][M : K_0]$ and the hypothesis of the theorem we see that the right hand-side of (6) tends to infinity as i tends to infinity. This completes the proof of Theorem 3.

5 Proof of Theorem 4

Let us recall the following well-known lemma.

Lemma 1 *Let F, K be number fields with $F \subseteq K$. Let $\wp$ be a prime ideal in $\mathcal{O}_F$. The following are equivalent:*
(i) $\wp$ ramifies totally in K.
(ii) $K = F(\alpha)$ for a root α of a $\wp$-Eisenstein polynomial in $\mathcal{O}_F[x]$.

Proof See for instance Theorem 24. (a) p.133 in [5]

We can now prove Theorem 4. Let $K_0 = K$ and for $i > 0$ let $K_i = K_{i-1}(\alpha_i)$. By assumption we have $p_i \nmid \Delta_{\mathbb{Q}(\alpha_j)}$ for $1 \leq j < i$. Since K_{i-1} is the compositum of $K_0, \mathbb{Q}(\alpha_1), ..., \mathbb{Q}(\alpha_{i-1})$ we conclude that only primes dividing $\Delta_{K_0}\Delta_{\mathbb{Q}(\alpha_1)}...\Delta_{\mathbb{Q}(\alpha_{i-1})}$ can ramify in K_{i-1}. By assumption we know that $p_i \longrightarrow \infty$ which implies that there is an i_0 such that $p_i \nmid \Delta_{K_{i-1}}$ for all $i \geq i_0$. Now we shift the index i by i_0 steps so that the new K_i, p_i, d_i are the old $K_{i+i_0}, p_{i+i_0}, d_{i+i_0}$ and therefore p_i is unramified in K_{i-1} for all $i \geq 1$. Now clearly $K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq ....$ and of course $\bigcup_{i=0}^{\infty} K_i = K(\alpha_1, \alpha_2, \alpha_3, ...)$. We will apply Theorem 3 but first we have to make sure that condition (3) holds.

Now let $i > 0$ and let M be an intermediate field with $K_{i-1} \subsetneq M \subseteq K_i$. Moreover set $m = [M : K_{i-1}]$. Let $\wp$ be any prime ideal in $\mathcal{O}_{K_{i-1}}$ above p_i. Since p_i is unramified in K_{i-1} we conclude that D_i is a $\wp$-Eisenstein polynomial in $\mathcal{O}_{K_{i-1}}[x]$. According to the Eisenstein criterion this implies that D_i is irreducible over K_{i-1} and since $K_i = K_{i-1}(\alpha_i)$ we get $[K_i : K_{i-1}] = d_i$. Moreover we conclude by Lemma 1 that $\wp$ ramifies totally in K_i/K_{i-1}. Let

$$(p_i) = \wp_1 ... \wp_s$$

be the decomposition into prime ideals in $\mathcal{O}_{K_{i-1}}$. Since $\wp_j$ ramifies totally in K_i/K_{i-1} it also ramifies totally in M/K_{i-1}. Hence

$$\wp_j = \mathfrak{B}_j^m$$

for $1 \leq j \leq s$ and prime ideals $\mathfrak{B}_j$ in $\mathcal{O}_M$. Let $\mathfrak{D}_{M/K_{i-1}}$ be the different of M/K_{i-1} (for the definition see [14] p.195). Then we have $\mathfrak{B}_j^{m-1} \mid \mathfrak{D}_{M/K_{i-1}}$ (see [14] (2.6) Theorem p.199) and therefore

$$(\mathfrak{B}_1 \ldots \mathfrak{B}_s)^{m-1} \mid \mathfrak{D}_{M/K_{i-1}}.$$

The discriminant $D_{M/K_{i-1}}$ is the norm of the different $\mathfrak{D}_{M/K_{i-1}}$ from M to K_{i-1} (see [14] (2.9) Theorem p.201). Taking then norms from K_{i-1} to $\mathbb{Q}$ we conclude

$$N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}) = N_{K_{i-1}/\mathbb{Q}}(N_{M/K_{i-1}}(\mathfrak{D}_{M/K_{i-1}})) = N_{M/\mathbb{Q}}(\mathfrak{D}_{M/K_{i-1}}).$$

Therefore

$$N_{M/\mathbb{Q}}((\mathfrak{B}_1 \ldots \mathfrak{B}_s)^{m-1}) \mid N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}}). \tag{7}$$

On the other hand we have

$$\begin{aligned} N_{M/\mathbb{Q}}((\mathfrak{B}_1 \ldots \mathfrak{B}_s)^{m-1}) &= (N_{M/\mathbb{Q}}(\prod_{j=1}^{s} \mathfrak{B}_j^{m}))^{\frac{m-1}{m}} = (N_{M/\mathbb{Q}}(\prod_{j=1}^{s} \wp_j))^{\frac{m-1}{m}} \\ &= (N_{M/\mathbb{Q}}(p_i))^{\frac{m-1}{m}} \qquad = p_i^{[K_{i-1}:\mathbb{Q}](m-1)}. \end{aligned}$$

Combining the latter with (7) and not forgetting that $1 < m = [M : K_{i-1}] \leq d_i$ we end up with

$$N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}})^{\frac{1}{[M:K_0][M:K_{i-1}]}} \geq p_i^{\frac{[K_{i-1}:\mathbb{Q}](m-1)}{[M:K_0]m}} = p_i^{\frac{[K_0:\mathbb{Q}](m-1)}{m^2}} \geq p_i^{\frac{1}{2m}} \geq p_i^{\frac{1}{2d_i}}.$$

By hypothesis of the theorem $p_i^{\frac{1}{d_i}}$ tends to infinity. Hence we can apply Theorem 3 and this completes the proof of Theorem 4.

6 Proof of Corollary 2

Since $H(p_i^{1/d_i}) = |p_i^{1/d_i}|$ we see that condition $|p_i^{1/d_i}| \longrightarrow \infty$ is necessary to obtain property (N). Now let us prove that this condition implies property (N). The hypothesis implies that there is an i_1 such that $p_j > d_j$ for all $j > i_1$. Therefore we have $p_i \geq p_j > d_j$ for all $i \geq j > i_1$. Clearly there exists an i_2 such that $p_i > \max\{d_1, ..., d_{i_1}\}$ for all $i \geq i_2$. Thus $p_i > \max\{d_1, ..., d_{i_1}, d_{i_1+1}, ..., d_i\}$ for all $i \geq i_0 := \max\{i_1, i_2\}$. This implies $p_i \nmid d_1 p_1 ... d_{i-1} p_{i-1}$ for all $i \geq i_0$. Set $D_i = x^{d_i} - p_i$, $\alpha_i = p_i^{1/d_i}$, $K_0 = K$ and $K_i = K(\alpha_1, ..., \alpha_i)$. Since $\Delta_{\mathbb{Q}(\alpha_j)}$ divides $|Disc(D_j)| = d_j^{d_j} p_j^{d_j - 1}$ we conclude $p_i \nmid \Delta_{\mathbb{Q}(\alpha_j)}$ for all $i \geq i_0$ and $1 \leq j < i$. Now shift the index by i_0 steps, more precisely: define $\widetilde{K}_i = K_{i_0+i}$, $\widetilde{p}_i = p_{i_0+i}$, $\widetilde{D}_i = D_{i_0+i}$, $\widetilde{d}_i = d_{i_0+i}$, $\widetilde{\alpha}_i = \alpha_{i_0+i}$. Hence $\widetilde{p}_i \nmid \Delta_{\mathbb{Q}(\widetilde{\alpha}_j)}$ for all i and $1 \leq j < i$. Clearly $K(\alpha_1, \alpha_2, \alpha_3, ...) = \widetilde{K}_0(\widetilde{\alpha}_1, \widetilde{\alpha}_2, \widetilde{\alpha}_3, ...)$ and $|\widetilde{p}_i^{1/\widetilde{d}_i}| \longrightarrow \infty$. Applying Theorem 4 with $K = \widetilde{K}_0$ and $\widetilde{p}_i, \widetilde{D}_i, \widetilde{d}_i, \widetilde{\alpha}_i$ completes the proof.

7 Proof of Theorem 5

Note that p_i^{1/d_i} and $p_i^{1/(d_i+1)}$ tend to infinity whereas $p_i^{1/(d_i^2+d_i)}$ is bounded as i tends to infinity. Hence Corollary 2 tells us that

$$L_1 = \mathbb{Q}(p_1^{1/d_1}, p_2^{1/d_2}, p_3^{1/d_3}, ...), \quad L_2 = \mathbb{Q}(p_1^{1/(d_1+1)}, p_2^{1/(d_2+1)}, p_3^{1/(d_3+1)}, ...)$$

both have property (N). But $p_i^{1/d_i}/p_i^{1/(d_i+1)} = p_i^{1/(d_i^2+d_i)}$ and so the compositum of L_1 and L_2 contains the field

$$\mathbb{Q}(p_1^{1/(d_1^2+d_1)}, p_2^{1/(d_2^2+d_2)}, p_3^{1/(d_3^2+d_3)}, ...)$$

which according to Corollary 2 does not have property (N). Therefore the compositum of L_1 and L_2 does not have property (N).

8 Proof of Corollary 3

For $i > 0$ the extension $F_i/\mathbb{Q}$ is generated by a root, say α_i, of a p_i-Eisenstein polynomial D_i in $\mathbb{Z}[x]$ (see Lemma 1 Section 5) of degree $d_i \leq d[F_0 : \mathbb{Q}]$. Therefore $F_i = \mathbb{Q}(\alpha_i)$ and the compositum of $F_0, F_1, F_2, F_3, ...$ is given by $F_0(\alpha_1, \alpha_2, \alpha_3, ...)$. From the hypothesis we know that $p_i \nmid \Delta_{\mathbb{Q}(\alpha_j)}$ for $1 \leq j < i$, in particular the primes p_i are pairwise distinct and thus $p_i^{1/d_i} \longrightarrow \infty$. Applying Theorem 4 yields the desired result.

9 Proof of Corollary 4

Write K_i for the compositum of $F_0, ..., F_i$. For $i > 0$ we have $1 \leq [K_i : K_{i-1}] \leq 3$, in particular K_i/K_{i-1} does not admit a proper intermediate field and so (3) simplifies to (4). By assumption there is a prime p_i which ramifies in F_i but not in F_j for $0 \leq j < i$. By virtue of (2) we conclude that

$$p_i^{[K_i:F_i]} \mid \Delta_{F_i}^{[K_i:F_i]} \mid \Delta_{K_i}.$$

On the other hand p_i does not ramify in $F_0, ..., F_{i-1}$ and so does not ramify in the compositum K_{i-1}, that is $p_i \nmid \Delta_{K_{i-1}}$. Appealing to (2) again we conclude

$$p_i^{[K_i:F_i]} \mid N_{K_{i-1}/\mathbb{Q}}(D_{K_i/K_{i-1}})$$

and therefore

$$N_{K_{i-1}/\mathbb{Q}}(D_{K_i/K_{i-1}})^{\frac{1}{[K_i:K_0][K_i:K_{i-1}]}} \geq p_i^{\frac{[K_i:F_i]}{[K_i:K_0][K_i:K_{i-1}]}}. \tag{8}$$

Since $[K_i : F_i] = [K_i : K_0]/[F_i : K_0]$ and $[F_i : K_0] \leq 3$ and $[K_i : K_{i-1}] \leq 3$ we see that the right hand-side of (8) is at least $p_i^{1/9}$. Now clearly $p_i \longrightarrow \infty$ as i tends to infinity and so the statement follows from Theorem 3.

10 Proof of Corollary 5

Note that the primes p_i are pairwise distinct. Hence there exists an integer $i_0 > 1$ such that $p_i > 3$ for all $i \geq i_0$. Write $\zeta_3 = (-1+\sqrt{-3})/2$ and define K_0 as the compositum of $\mathbb{Q}(\zeta_3), F_1^{(g)}, ..., F_{i_0}^{(g)}$ and for $i > 0$ define K_i as the compositum of $K_0, F_1^{(g)}, ..., F_i^{(g)}$. Now $\Delta_{\mathbb{Q}(\zeta_3)} = -3$ and using our assumption we conclude that $p_i \nmid \Delta_{K_{i-1}}$ for all $i \geq i_0$. We will show that for $i \geq i_0$ the prime p_i ramifies in M for each intermediate field $K_{i-1} \subsetneq M \subseteq K_i$. By similar arguments as in the proof of Corollary 4 we derive

$$N_{K_{i-1}/\mathbb{Q}}(D_{M/K_{i-1}})^{\frac{1}{[M:K_0][M:K_{i-1}]}} \geq p_i^{\frac{1}{18}}.$$

Applying Theorem 3 proves the statement. So let us now prove that p_i ramifies in M. If (a) holds we have $M = K_i$ and since $p_i \mid \Delta_{F_i} \mid \Delta_{K_i}$ we are done. Next suppose (b) holds. Since ζ_3 lies in K_0 we have $[K_i : K_{i-1}] \leq 3$ and so $M = K_i$ as before. Now suppose (a) does not hold. Then $F_i^{(g)}/\mathbb{Q}$ must have Galois group isomorphic to S_3. The unique quadratic subfield, let us call it E_i, is then given by $\mathbb{Q}(\sqrt{Disc(D)})$ where D is the minimum polynomial of any α with $F_i = \mathbb{Q}(\alpha)$. Note that $[K_i : K_{i-1}] = [K_{i-1}F_i^{(g)} : K_{i-1}] = [K_{i-1}F_i^{(g)} : K_{i-1}E_i][K_{i-1}E_i : K_{i-1}] \leq [F_i^{(g)} : E_i][E_i : \mathbb{Q}] = 3 \cdot 2$. Hence if K_i/K_{i-1} has Galois group isomorphic to S_3 then each strict intermediate field of K_i/K_{i-1} is either the compositum of K_{i-1} and a conjugate field of $F_i/\mathbb{Q}$ or the compositum of K_{i-1} and E_i. Since p_i ramifies in all conjugate fields of $F_i/\mathbb{Q}$ it remains to show that p_i ramifies in E_i. Suppose (c) holds. Write Q for the largest square dividing $Disc(D_\alpha)$ and set $A = Disc(D_\alpha)/Q$. Then $p_i \mid A$ and $A \mid \Delta_{E_i}$. In particular p_i ramifies in E_i. Now suppose (d) holds. By Corollary 1 of [17] we see that in this case $F_i^{(g)}/E_i$ is unramified at all finite primes. Since p_i ramifies in $F_i^{(g)}$ it must already ramify in E_i. This shows that for $i \geq i_0$ the prime p_i ramifies in M for each intermediate field $K_{i-1} \subsetneq M \subseteq K_i$ and thereby completes the proof.

11 Some applications of the Northcott property

Applications to algebraic dynamics were a motivation for Northcott to study heights and related finiteness properties. Let S be a set and let $f : S \longrightarrow S$ be a self map of S. When we iterate this map we obtain an orbit $O_f(\alpha)$ for each point $\alpha \in S$

$$O_f(\alpha) = \{\alpha, f(\alpha), f \circ f(\alpha), f \circ f \circ f(\alpha), ...\}.$$

We say a point α in S is a preperiodic point under f if $O_f(\alpha)$ is a finite set. We are interested in the case where $S = \overline{\mathbb{Q}}$ and f is a polynomial map. An important problem is to decide whether there are finitely many preperiodic points (under f) in a given subset T of S. A more specific version was proposed by Dvornicich and Zannier ([4] Question): *let T be a subfield of $\overline{\mathbb{Q}}$ and let $f \in T[x]$ be a polynomial map with* $\deg f \geq 2$. *Can one decide whether the set of preperiodic points in T (under f) is finite or infinite?* If T is the cyclotomic closure of a number field Dvornicich and Zannier's Theorem 2 in [3] positively answers the question by explicitly describing all polynomials $f \in T[x]$ with infinitely many preperiodic points and $\deg f \geq 2$. If T has property (N) the situation is much simpler and a well-known argument due to Northcott (see [16] Theorem 3) answers the question in the affirmative.

Theorem 6 (Northcott) *Suppose T is a subset of $\overline{\mathbb{Q}}$ with property (N) and suppose $f \in \overline{\mathbb{Q}}[x]$ with $\deg f \geq 2$. Then T contains only finitely many preperiodic points under f.*

Proof For each non-zero rational function $g \in \overline{\mathbb{Q}}(x)$ there exists a positive constant $b_g < 1$ such that $H(g(\alpha)) \geq b_g H(\alpha)^{\deg g}$ for all $\alpha \in \overline{\mathbb{Q}}$ and α not a pole of g (see [4] or [9] Proposition 1). We apply this inequality with $g = f$. Suppose α is preperiodic under the polynomial f and $H(\alpha) > 1/b_f^2 > 1$. Hence $H(f(\alpha)) \geq b_f H(\alpha)^{\deg f} > H(\alpha)^{\deg f - 1/2} \geq H(\alpha)^{3/2}$. Thus with f^n the n-th iterate of f we get $H(f^n(\alpha)) > H(\alpha)^{(3/2)^n} > 1$ which is a contradiction for n large enough. Therefore $H(\alpha) \leq 1/b_f^2$ and since T has property (N) this proves the lemma.

Using our results on property (N) we get, presumably new, answers on Dvornicich and Zannier's question.

In [11] Narkiewicz introduced the so-called property (P) for fields. A field F has the property (P) if for every infinite subset $\Gamma \subset F$ the condition $f(\Gamma) = \Gamma$ for a polynomial $f \in F[x]$ implies $\deg f = 1$. Narkiewicz proposed several problems involving property (P), e.g. the analogue of Bombieri and Zannier's question ([12] Problem 10 (i)): *does $\mathbb{Q}^{(d)}$ have property (P)?* Or less specifically ([13] Problem XVI): *give a constructive description of fields with property (P).* Dvornicich and Zannier have noticed ([3] p. 534) that for subfields of $\overline{\mathbb{Q}}$ property (N) implies property (P) (see also [4] Theorem 3.1 for a detailed proof). Hence an affirmative answer on Bombieri and Zannier's question would also positively answer Narkiewicz's first problem, and the explicit examples of fields with property (N) shed some light on Narkiewicz's second problem. But property (P) does not imply property (N) as shown in [3] Theorem 3. However, Dvornicich and Zannier also remarked ([3] p. 533 and [4] Proposition 3.1) that the property (P) already implies the finiteness of the set of preperiodic points under a polynomial map of degree at least 2. Kubota and Liardet [7] proved the existence and Dvornicich and Zannier ([3] Theorem 3) gave explicit examples of fields with property (P) that cannot be generated over $\mathbb{Q}$ by algebraic numbers of bounded degree. These examples refuted a conjecture of Narkiewicz ([13] p.85). Corollary 2 provides further examples of such fields but, opposed to Dvornicich and Zannier's example, they also have property (N).

Acknowledgements The author would like to thank Professor Umberto Zannier for sending him a preprint of [4] and the referee for the example just after Theorem 5 and other valuable comments which improved the exposition of this article.

References

1. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
2. E. Bombieri and U. Zannier, *A Note on heights in certain infinite extensions of* $\mathbb{Q}$, Rend. Mat. Acc. Lincei **12** (2001), 5–14.
3. R. Dvornicich and U. Zannier, *Cyclotomic Diophantine problems*, Duke Math. J. **139** (2007), 527–554.
4. ———, *On the properties of Northcott and Narkiewicz for fields of algebraic numbers*, Functiones et Approximatio **39** (2008), 163–173.
5. A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge University Press, 1991.
6. D. Hilbert, *The Theory of Algebraic Number Fields*, Springer, 1998.

7. K. K. Kubota and P. Liardet, *Réfutation d'une conjecture de W. Narkiewicz*, C. R. Acad. Sci. Paris **282** (1976), A1261–A1264.
8. S. Lang, *Algebraic Number Theory*, Springer, 1994.
9. P. Liardet, *Sur les transformations polynomiales et rationnelles*, Sm. Th. Nomb. Bordeaux **1** (1971-1972).
10. D. A. Marcus, *Number Fields*, Springer, 1977.
11. W. Narkiewicz, *On polynomial transformations*, Acta Arith **7** (1961/1962), 241–249.
12. ———, *Some unsolved problems*, Mem. Soc. Math. Fr. **25** (1971), 159–164.
13. ———, *Polynomial Mappings*, Lecture Notes in Mathematics 1600, Springer, 1995.
14. J. Neukirch, *Algebraic Number Theory*, Springer, 1999.
15. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Phil. Soc. **45** (1949), 502–509 and 510–518.
16. ———, *Periodic points on an algebraic variety*, Ann. of Math. **51** (1950), 167–177.
17. H. Osada, *The Galois groups of polynomials* $X^n + aX^l + b$, J. Number Theory **25** (1987), 230–238.
18. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.