*Functiones et Approximatio*
*XXXIX.1 (2008), 163–173*

# ON THE PROPERTIES OF NORTHCOTT AND OF NARKIEWICZ FOR FIELDS OF ALGEBRAIC NUMBERS

Roberto Dvornicich, Umberto Zannier

We dedicate this paper to
Professor Władysław Narkiewicz
on the occasion of his 70-th birthday

**Abstract:** This paper surveys on some recent results concerning certain finiteness properties for subfields $K$ of $\overline{\mathbb{Q}}$: first, the so-called *Northcott property* of finiteness of elements in $K$ of bounded Weil height and then the *Property (P)* of finiteness of possible subsets of $K$ sent onto themselves by some polynomial of degree $> 1$. The first was established by Northcott for the union of the fields of given degree over $\mathbb{Q}$; the second one was introduced by Narkiewicz; it is also related to preperiodic points for polynomial maps. It is known that the first implies the second, so they both hold for number fields. As to fields of infinite degree over $\mathbb{Q}$, we shall see some criteria for the first property, and hence for the second, but we shall also see that the second property does not imply the first. Some of these constructions provide answers, both in the positive and in the negative as the case may be, to questions explicitly formulated by Narkiewicz.
**Keywords:** Field Arithmetic, Preperiodic points

## 1. Introduction

This paper surveys on some recent results concerning certain finiteness properties in the context of fields $K$ of algebraic numbers. We shall first consider the so-called *Northcott property* of finiteness of elements in $K$ of bounded Weil height and then the *Property (P)* of finiteness of possible subsets of $K$ sent onto themselves by some polynomial of degree $> 1$. The first property was established by Northcott for number fields and actually for the union of the fields of given degree over $\mathbb{Q}$; the second one was introduced and first investigated by Narkiewicz; it is also related to the structure and fields of definition of the preperiodic points for polynomial maps.

As we shall recall with proof, these properties are linked, since the first implies the second. In particular, they both hold for number fields. Therefore we shall usually consider fields of infinite degree over $\mathbb{Q}$; we shall see some criteria which guarantee the first property, and hence the second, but we shall also see examples which show that the second property does not imply the first.

**2000 Mathematics Subject Classification:** 11G10.

It turns out that some of these constructions provide answers, both in the positive and in the negative as the case may be, to questions explicitly formulated by Narkiewicz.

Although we shall not give full details of the arguments, we shall try to present the main points of the methods and to give occasionally partial proofs or illustration of special cases.

## 2. The Northcott property

To introduce this property we first briefly recall the definition and a few important facts about the Weil (logarithmic) height on $\overline{\mathbb{Q}}$, referring to [1] for proofs. Let $k$ be a number field and let $M_k$ be the set of places of $k$, i.e., equivalence classes of absolute values, normalized so to extend the usual absolute values of $\mathbb{Q}$. (Namely, for $x \in \mathbb{Q}$, $|x|_v$ equals the usual absolute value if $v$ is archimedean whereas $|p|_v = p^{-1}$ if $v$ lies above $p$.) For $v \in M_k$ let $k_v$ be a completion of $k$ with respect to $v$; it is a finite extension of the completion $\mathbb{Q}_v$ of $\mathbb{Q}$ with respect to the induced place of $\mathbb{Q}$. Then, letting $\log^+ t := \log \max(1, t)$, for an $x \in k$ we set

$$h(x) = [k : \mathbb{Q}]^{-1} \sum_{v \in M_k} [k_v : \mathbb{Q}_v] \log^+ |x|_v.$$

It turns out that this does not depend on $k$, so it defines a real function on $\overline{\mathbb{Q}}$.[1] For a rational fraction $x = p/q$ in lowest terms we have $h(x) = \log \max(|p|, |q|)$. Also, we have the properties

(Hi) $h(x) \geq 0$ with equality if and only if $x$ is $0, \infty$ or a root of unity.

(Hii) $h(x^\sigma) = h(x)$ for any automorphism $\sigma$ of $\overline{\mathbb{Q}}$.

(Hiii) $h(x^m) = |m| h(x)$ for $m \in \mathbb{Q}$.

(Hiv) $h(x_1 + \ldots + x_r) \leq h(x_1) + \ldots + h(x_r) + \log r$.

(Hv) $h(xy) \leq h(x) + h(y)$.

These properties express in particular a 'good' behavior of $h$ with respect to algebraic operations. For future reference we add a further important property in this respect:

(Hvi) Let $R \in \overline{\mathbb{Q}}(X)$ be a rational function. For $x \in \overline{\mathbb{Q}}$ we have $h(R(x)) = \deg(R)\ h(x) + O(1)$, where the implied constant depends only on $R$.

**Definition 2.1.** *We say that a subset $F \subset \overline{\mathbb{Q}}$ has the Northcott property or the Property (N) if for any $B$ the set of $x \in F$ with $h(x) \leq B$ is finite.*

This terminology comes from the paper [3]. We shall usually consider only the case when $F$ is a field. Note that $\mathbb{Q}$ has trivially the Property (N), because $h(p/q) = \log \max(|p|, |q|)$ for $p, q$ coprime integers. The well-known *Northcott Theorem*, which has many useful diophantine applications, asserts that the union of the fields of degree $\leq d$ over $\mathbb{Q}$ has the Property (N), for every integer $d$. The proof is easy and actually yields the following more general statement:

[1] There is also a natural extension to $\mathbb{P}_1(\overline{\mathbb{Q}})$ by setting $h(\infty) = 0$.

**Theorem 2.1.** *Let $F \subset \overline{\mathbb{Q}}$ be a field with the Property (N) and let $d$ be a positive integer. Then the set of algebraic numbers of degree at most $d$ over $F$ has the Property (N). In particular, every finite extension of $F$ has the Property (N).*

**Proof.** Let $B$ be a real number and let $x$ be an algebraic number with $h(x) \leq B$ and $[F(x) : F] \leq d$. If $y$ is any conjugate of $x$ over $F$ we have $h(y) = h(x) \leq B$, in view of property (Hii) above. There are at most $d$ such conjugates, hence if $s$ is any elementary symmetric function of them we easily derive from (Hiii) and (Hiv) that $h(s) \leq d2^d B + d$. Therefore the heights of the coefficients of the minimal polynomial of $x$ over $F$ are bounded. Since $F$ has the Property (N), such coefficients have only finitely many possibilities, and since the number of coefficients is bounded by $d$, the minimal polynomial lies in a finite set. Hence the same holds for $x$, proving the theorem. ■

**Corollary 2.1 (Northcott Theorem).** *There are only finitely many algebraic numbers of bounded height and degree. In other words, the union of the number fields of degree $\leq d$ has the Property (N). In particular, every number field has the Property (N).*

Note that of course the field of all algebraic numbers has not the Property (N); and for instance the maximal cyclotomic extension $\mathbb{Q}^c$ of $\mathbb{Q}$ already has not the Property (N), since every root of unity $\zeta$ has $h(\zeta) = 0$. This big cyclotomic field and certain of its subfields will be an important source for many of the examples below.

It may be of interest, both for its own sake and also in view of the many applications of the Northcott property, to produce examples of fields of algebraic numbers other than number fields possessing it; *a priori* there might be no such field, i.e., with the Property (N) and infinite degree over $\mathbb{Q}$. In this direction, for instance, a question which Corollary 2.1 suggests naturally is whether the Property (N) holds for the *composite* of the fields of degree $\leq d$, rather that for the *union* of such fields. In other words, we ask whether any field generated by elements of bounded degree has the Northcott property. For general $d$ we do not know the answer to this question. However, in the paper [3] the following result was established:

**Theorem BZ.** Let $k$ be a number field and let $k_{ab}^{(d)}$ be the composite of all abelian extensions of $k$ of degree $\leq d$. Then $k_{ab}^{(d)}$ has the Property (N).

Note that every quadratic extension is abelian, so in particular this answers affirmatively the above question for $d = 2$. We now give in detail the simple proof of the special case $k = \mathbb{Q}$, $d = 2$ of this theorem. The general proof relies on similar principles but is more complicated; for it, we refer to the paper [3] or to the book [1].

**Proof of the special case $k = \mathbb{Q}$, $d = 2$ of Theorem BZ.** We have to prove that the field $K$ obtained by adding to $\mathbb{Q}$ the square roots $\sqrt{p}$ of prime numbers has the Property (N). For a set $R$ of primes we denote by $K_R$ the field obtained by

adding to $\mathbb{Q}$ the square roots $\sqrt{p}$ for $p \in R$. So, $K$ is the union of the $K_R$ for finite sets $R$ of primes.

Let $l > 2$ be a prime which does not lie in the finite set $R$ and put $S = R \cup \{l\}$. Every element $x \in K_S$ may be written uniquely as $x = t + u\sqrt{l}$, $t, u \in K_R$. Denoting with an accent conjugation over $K_R$, we have $x' = t - u\sqrt{l}$. Hence, by (Hii), (Hiv) above we have

$$h(2u\sqrt{l}) = h(x - x') \leq h(x) + h(x') + \log 2 \leq 2h(x) + \log 2. \tag{2.1}$$

Let $w$ run through the places of $K_S$ above $l$ (normalized so to extend those on $\mathbb{Q}$). Suppose $u \neq 0$, i.e., $x \notin K_R$. Then, since $l$ ramifies in $K_S$ but not in $K_R$, we have that $w(2u)$ is an integer, whereas $w(\sqrt{l}) = 1/2$. Hence, $|w(2u\sqrt{l})| \geq 1/2$ and therefore $|\log |2u\sqrt{l}|_w| \geq (\log l)/2$. Now, for any $y \in K_S$ we have

$$h(y) \geq [K_S : \mathbb{Q}]^{-1} \sum_{w|l} [(K_S)_w : \mathbb{Q}_l] \log^+ |y|_w,$$

$$h(y) = h(y^{-1}) \geq [K_S : \mathbb{Q}]^{-1} \sum_{w|l} [(K_S)_w : \mathbb{Q}_l] \log^+ |y^{-1}|_w.$$

Hence on summing and using $|\log \xi| = \log^+ \xi + \log^+ \xi^{-1}$ for $\xi > 0$, we obtain

$$2h(y) \geq [K_S : \mathbb{Q}]^{-1} \sum_{w|l} [(K_S)_w : \mathbb{Q}_l] |\log |y|_w|.$$

We apply this inequality with $y = 2u\sqrt{l}$. Recalling $|\log |2u\sqrt{l}|_w| \geq (\log l)/2$, $\sum_{w|l} [(K_S)_w : \mathbb{Q}_l] = [K_S : \mathbb{Q}]$ and recalling (2.1) we get

$$8h(x) + 4 \log 2 \geq \log l.$$

Suppose now that $h(x) \leq B$. Then $\log l \leq 8B + 4 \log 2$. We deduce that if $x \in K_S$ then either $l \leq 16e^{8B}$ or $x$ must lie in $K_R$. We conclude that $x$ lies in $K_T$, where $T = T_B$ is the finite set of primes $l \leq 16e^{8B}$. Hence if $x \in K$ and $h(x) \leq B$, then $x$ lies in the number field $K_T$ which depends only on $B$. By Northcott Theorem, $x$ has only finitely many possibilities, concluding the argument. ∎

## 3. The Property (P)

In [7] Narkiewicz introduced the following definition.

**Definition 3.1.** *We say that 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* $\deg f = 1$.

Note that, like for the Property (N), we could formulate the property for subsets $F$ of a field; Narkiewicz also introduced a similar property (denoted (SP)) involving polynomials in several variables satisfying suitable assumptions. We shall not be concerned here with these more general concepts and also we shall mostly work with subfields $F$ of $\overline{\mathbb{Q}}$.

Note that letting $f$ in Definition 3.1 have coefficients in any field $F' \supset F$ would plainly lead to an equivalent notion, since the condition $f(R) \subset F$ for a set $R \subset F$ with $\#R > \deg f$ implies $f \in F[X]$. Further, note that a polynomial of degree 1 over $F$ induces a bijective map $f : F \to F$, so the implication $\deg f = 1$ is the best that we can generally expect from the assumption $f(\Gamma) = \Gamma$.

In this paper, sets $\Gamma$ with $f(\Gamma) = \Gamma$ will be said *invariant* for $f$.[2] We can obtain some invariant sets by means of *periodic* points, widely studied in the context of dynamical systems (see [6]); we recall here the definition:

**Definition 3.2.** *We say that a point $x \in F$ is periodic for a map $\varphi : F \to F$ if for some integer $n > 0$ we have $\varphi^{(n)}(x) = x$, where $\varphi^{(n)}$ denotes the $n$-th iterate. We say that $x$ is preperiodic if $\varphi^{(m)}(x)$ is periodic for some $m \geq 0$.*

Note that if $x$ is periodic for a map $\varphi$, then the set $\{\varphi^{(r)}(x) : r \in \mathbb{N}\}$ is invariant for $\varphi$. Then we have the following simple observation:

**Proposition 3.1.** *If a field $F$ has the Property (P), every polynomial $f$ of degree $> 1$ has only finitely many preperiodic points in $F$.*

**Proof.** Let $\Omega$ be the set of preperiodic points in $F$ for the polynomial $f \in F[X]$, of degree $> 1$. If $x \in \Omega$ the sequence of forward images $f^{(r)}(x)$, $r = 0, 1, \ldots$, eventually consists of a full period of a periodic point $y$ for $f$; we then say that '$x$ belongs to $y$'.

Now, let $\Omega$ be infinite; then, either the set of periodic points for $f$ is infinite or there exist infinitely many points $x \in \Omega$ belonging to a same periodic point $y$.

In the first case we let $\Gamma$ be the infinite set of periodic points in $\Omega$; it plainly satisfies $f(\Gamma) = \Gamma$ because if $z$ is periodic for $f$ of period $n$ we have $z = f(f^{(n-1)}(z)) \in f(\Gamma)$ and $f(z) \in \Gamma$. Hence $F$ has not the Property (P).

In the second case, let $\Omega_y$ be the infinite set of preperiodic points belonging to $y$. Let us consider finite sequences $y_0, y_1, \ldots, y_h$ of elements $y_j \in \Omega_y$ such that $y_0$ is in the period of $y$, $y_1$ is not periodic and $f(y_j) = y_{j-1}$ for $j > 0$; we call such a sequence a *path*; observe that in a path we have $y_i \neq y_j$ for $i \neq j$. Note that the sequence of forward images of any element $z \in \Omega_y$ yields a subsequence that is a path: it suffices to omit all periodic elements in it except the first. Then, since $\Omega_y$ is infinite we may find infinitely many paths with the same $y_0$. And since the equation $f(X) = y_0$ has at most $\deg f$ solutions, there exists an infinite set of paths with the same $y_0, y_1$; and then by repeating the argument with $y_1$ in place of $y_0$ we see that there exist infinitely many paths with the same $y_0, y_1, y_2$. And so on, iterating this argument we can construct an *infinite* path $y_0, y_1, \ldots$. Plainly the set $\Gamma = \{y_0, y_1, \ldots\} \cup \{f^{(n)}(y_0) : n \in \mathbb{N}\}$ is infinite and violates the Property (P). This proves the proposition. ∎

*Some examples.* The idea beyond the Property (P) is that if $\Gamma$ is an invariant set and $\gamma \in \Gamma$, not only we must have $f(\gamma) \in \Gamma$ but also there must exist $\gamma' \in \Gamma$ such that $f(\gamma') = \gamma$. It is this last requirement which gives a more severe restriction,

[2] For other authors, sometimes 'invariant' means just $f(\Gamma) \subset \Gamma$.

because if $\deg f > 1$ we may expect that solving the equation $f(X) = \gamma$ brings us actually out not just of $\Gamma$ but of the whole field we are working with. Needless to say, this rough expectation can possibly apply only for fields with somewhat strong 'rationality restrictions'. Indeed, let us see some examples of fields without Property (P).

Neither $\overline{\mathbb{Q}}$ nor its maximal real subfield $\overline{\mathbb{Q}} \cap \mathbb{R}$ have the Property (P): it suffices to observe that this whole real field is invariant for every polynomial of odd degree with coefficients in it. For a prime $p > 2$, it is easily seen that $\mathbb{Z}_p^*$ is invariant for every polynomial $X^l$ for $l$ coprime to $p(p-1)$; hence $\mathbb{Q}_p$ has not the Property (P). The maps $x \mapsto x^l$ also show that the maximal cyclotomic field $\mathbb{Q}^c$ has not the Property (P).[3] Note that the roots of unity are preperiodic for any of these maps. An example related to but less evident than this last one is the maximal real subfield $\Re\mathbb{Q}^c$ of $\mathbb{Q}^c$. To see it does not have the Property (P), consider for instance the set $\Gamma := \{2\Re\zeta = \zeta + \zeta^{-1}\}$ for $\zeta$ running through the roots of unity, so $\Gamma$ is an infinite subset of $\Re\mathbb{Q}^c$. Let now $T_d$ be the Chebishev polynomial of degree $d$: it is the unique polynomial such that $T_d(X + X^{-1}) = X^d + X^{-d}$. Note that $\Gamma$ is invariant for any $T_d$, which proves the previous claim. We shall see that inside $\mathbb{Q}^c$ essentially (i.e., up to suitable normalization) these are the only examples of infinite invariant sets for polynomials of degree $> 1$.

As to fields *with* the Property (P), a source of examples comes from fields with the Property (N). In fact we have the following

**Theorem 3.1.** *For a subfield $F$ of $\overline{\mathbb{Q}}$ the Property (N) implies the Property (P).*

**Proof.** Let $F$ be a field of algebraic numbers with the Property (N), let $f \in F[X]$ have degree $d > 1$ and let $\Gamma \subset F$ be invariant for $f$. Our task is to prove that $\Gamma$ cannot be infinite.

By property (Hvi) of the Weil height, there exists a number $B = B_f > 0$ such that $h(f(x)) > dh(x) - B$ for every algebraic number $x$. We deduce that if $h(x) \geq 2B$ then $h(f(x)) > gh(x) \geq 2B$, where $g := d - (1/2) \geq 3/2$. By iteration we see that if $h(x) \geq 2B$ then $h(f^{(m)}(x)) > g^m h(x)$ for any integer $m > 0$.

Now, let $y \in \Gamma$. Since $f(\Gamma) = \Gamma$ we can form an infinite sequence $y_0 = y, y_1, \ldots$, such that $f(y_j) = y_{j-1}$. We contend that $h(y_m) < 2B$ for all large enough $m$. In fact, if $h(y_m) \geq 2B$ we deduce from the above (taking $x = y_m$) that $h(y) > g^m h(y_m) \geq 2g^m B$, which cannot hold for large $m$. Hence, since $F$ has the Property (N), there are only finitely many $y_j$. Hence there exist $r < s$ arbitrarily large and such that $y_r = y_s$. This means that $y = y_0$ belongs to the period $\{y_s, y_{s-1}, \ldots, y_r\}$ and in particular $h(y) < 2B$. Hence $\Gamma$ consists of elements in $F$ with Weil height bounded by $2B$ and is therefore a finite set, as asserted. ∎

This result also follows from the general properties proved in [8, Chap. IX].

As we shall point out later, there is no general converse implication (as shown in [4]).

[3] Note that $\mathbb{Q}^c$ is Hilbertian, as shown by Weissauer – see also [4]. This may be considered a 'rationality restriction', yet not sufficient for the Property (P).

Combining this result with Corollary 2.1 we obtain the well-known fact that every number field has the Property (P) (see [8]). Moreover, Theorem BZ gives some fields of infinite degree over $\mathbb{Q}$ having the Property (P). In particular, the special case $k = \mathbb{Q}$, $d = 2$ of Theorem BZ yields:

**Theorem 3.2.** *The field* $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots)$ *has the Property (P).*

This answers in the affirmative the Open Question XVII in [8, p. 69].

As Proposition 3.1 shows, there is a link between the validity of Property (P) for a field $k$ and the existence of infinitely many preperiodic points defined over $k$ for a polynomial map $f(x) \in k[x]$ of degree $> 1$. More generally, one can investigate the field of definition of such preperiodic points. For instance, it is well-known that there can be only finitely many preperiodic points for $f$ of bounded degree over $\mathbb{Q}$ (see for instance [8]). However, for a field of algebraic numbers of infinite degree not much seems to be known, and the following vague question seems to be widely open:

**Question.** Let $F$ be a subfield of $\overline{\mathbb{Q}}$ and $f(x) \in F[x]$ be a polynomial map of degree $> 1$. Denote by $\Pi_f(F)$ the set of preperiodic points for $f$ contained in $F$. Can one decide whether $\Pi_f(F)$ is finite or infinite?

For the case when $F = k^c$, the cyclotomic closure of a number field $k$ in $\bar{k}$, in [4] we have developed a method for explicitly answering this question. As we shall see, this throws more light on the possibility that Property (P) may hold for fields of infinite degree over $\mathbb{Q}$ and allows us to answer a couple of more questions raised by Narkiewicz.

To start with, as observed above, $\Pi_f(k^c)$ may in fact be infinite, in view of the monomial maps $x \mapsto \zeta x^d$, where $\zeta$ is any root of unity and $d$ is any integer $\geq 2$. On the other hand, using some equidistribution results (see [2]), one can prove that if a polynomial map $f$ contains infinitely preperiodic points that are roots of unity, then $f$ must be a monomial. In fact, the quoted results imply that the set of Galois conjugates of a preperiodic point "tends to be" uniformly distributed in $\mathbb{C}$ "around" the whole Julia set of $f$, as the degree of the point tends to $\infty$. Therefore, if there were infinitely many preperiodic roots of unity, the unit circle would be $f$-invariant. But it is an easy exercise to show that a polynomial leaving the unit circle invariant is necessarily a monomial.

It turns out, however, that there exist polynomial maps with infinitely many preperiodic points other than the roots of unity; more than this, in [4] we are in fact able to classify all polynomial maps $f$ of degree $> 1$ for which $\Pi_f(k^c)$ is infinite. We show that there are essentially two cases:

**Theorem DZ.** (For a proof we refer to [4].) Let $f \in k[x]$ be a polynomial of degree $d \geq 2$. Then $\Pi_f(k^c)$ is finite unless for some polynomial $L \in \overline{\mathbb{Q}}[x]$ of degree 1 and for some $\epsilon = \pm 1$, $(L \circ f \circ L^{-1})(x)$ is either $(\epsilon x)^d$ or $T_d(\epsilon x)$.

Here $T_d(x)$ denotes, as usual, the $d$-th Chebishev polynomial: it is the unique polynomial satisfying the identity $T_d(x + x^{-1}) = x^d + x^{-d}$. We recall that both

$x^d$ and $T_d(x)$ have the same parity of $d$; this fact allows to remove the "$\epsilon$" except when $d$ is odd and we are in the "Chebishev case".

It is to be remarked that the linear polynomial $L$ need not be defined over $k$; however, it can be proved that it may be chosen over a certain radical extension of $k$ (actually a quadratic one in the "Chebishev case").

We also note that the exceptional cases of the theorem are genuine exceptions to finiteness. In fact, the finiteness property is preserved under conjugation by polynomials of degree 1, so it suffices to check that $(\epsilon x)^d$ and $T_d(\epsilon x)$ have infinitely many preperiodic points in $\mathbb{Q}^c$, which is straightforward. (The nonzero preperiodic points are just roots of unity in the first case and numbers of the form $\zeta + \zeta^{-1}$, $\zeta$ a root of unity, in the second case.)

We now come back to the study of Property (P). First of all note that Proposition 3.1 immediately implies the following well-known result:

**Corollary 3.1.** *The cyclotomic extension $K = k^c$ does not have the property (P).*

Next, consider the Open Question XV in [8]: *Is the Property (P) preserved under finite extensions?*

With the methods developed in [4] for the proof of Theorem DZ above, we can answer this question in the negative, by producing an explicit example of a field $K$ of algebraic numbers, of infinite degree over $\mathbb{Q}$, having the Property (P), and a finite extension $K'$ of $K$ not having the Property (P).

Hence, in view of Theorem 2.1, this example settles at the same time, again in the negative, the question of whether Property (N) and Property (P) are equivalent.

Our results can be collected in the following statement:

**Theorem 3.3.** *Let $p$ be a prime such that $p-1$ has an odd prime factor $l$. Let $K'$ be the field generated over $\mathbb{Q}$ by the roots of unity of $p$-power order and let $K$ be the unique subfield of $K'$ such that $[K' : K] = l$. Then:*

*(i) $K$ has the Property (P);*
*(ii) $K'$ has not the Property (P);*
*(iii) $K$ has not the Property (N).*

We remark that $Gal(K'/\mathbb{Q}) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_p \times \mathbf{F}_p^*$, so that this Galois group has in fact a unique subgroup of order $l$, corresponding to $K$.

Another feature of the field $K$ is that it cannot be generated over $\mathbb{Q}$ by elements of bounded degree. This follows from the structure of the Galois group. (The mere existence of a such a field with Property (P) was established in a less direct way by K. Kubota and P. Liardet; see [8, p. 85].) As for the Property (N), it would be interesting to know whether there exists such a field without the Property (P).

Theorem 3.3 is just an instance of what can be said and it could be easily generalized or varied in many ways. In fact, Theorem 3.3 results from a complete classification of polynomials $f \in k^c[x]$ of degree $d \geq 2$ and infinite invariant sets $\Gamma$ for $f$, $\Gamma \subset k^c$. This classification in turn can be obtained by using the same methods used in proving Theorem DZ, and in practice gives the precise obstructions

for $k^c$ to have the property (P). With reference to Theorem 2* and Proposition 1 of [4], we restate without proof this classification as follows:

**Proposition 3.2.** *Let $f(x) \in k[x]$ be a polynomial map of degree $\geq 2$ and $\Gamma \subset k^c$ be an infinite set such that $f(\Gamma) = \Gamma$. Then $f$ is of one of the two types described in Theorem DZ. Corresponding to these two cases, we have, denoting by $U$ the set of roots of unity in $\overline{\mathbb{Q}}$:*

*(a) if $f = L^{-1} \circ (\epsilon x)^d \circ L \in k[x]$, then $L(\Gamma)$ is contained in $\{0\} \cup U$;*

*(b) if $f = L^{-1} \circ T_d(\epsilon x) \circ L \in k[x]$, then $L(\Gamma)$ is contained in $\{u + u^{-1} | u \in U\}$.*

**Proof of Theorem 3.3 (assuming Prop. 3.2).** Preliminary to the proof we note that the only roots of unity contained in $K$ are $\pm 1$: in fact, it is standard that the possible order of roots of unity in $K'$ divides $2p^r$ for some $r$. Hence if $K$ contains a root of unity of order $> 2$ it contains a primitive $p$-th root of unity. But this is not fixed by the Galois subgroup of order $l$.

We start by proving (i), namely that $K$ has the Property (P).

We argue by contradiction and suppose that $f \in K[x]$ has degree $d \geq 2$ and that $\Gamma$ is an infinite subset of $K$ such that $f(\Gamma) = \Gamma$. Since $K \subset \mathbb{Q}^c$, Proposition 3.2 says that we only have two cases two consider.

(a) $L(\Gamma) \subset \{0\} \cup U$, where $L(x) = ax + b$ for some algebraic numbers $a, b$, $a \neq 0$. Therefore, for some algebraic numbers $A, B$, $A \neq 0$, we have $A\zeta + B \in K$ for infinitely many $\zeta \in U$.

Choose now any $\sigma \in G_K := Gal(\overline{K}/K)$; conjugating we obtain

$$A\zeta - A^\sigma \zeta^\sigma + (B - B^\sigma) = 0. \tag{3.1}$$

For fixed $\sigma$ we view this as a linear relation among roots of unity, using the results and the terminology of [5].

Suppose first that $B \notin K$, so $B - B^\sigma \neq 0$ for a suitable $\sigma$. Then (3.1) is a *normalized relation* (in the sense that there is a nonzero constant term $B - B^\sigma$ and that there is no proper vanishing subsum). Hence [5] implies that there are only finitely many solutions, a contradiction. Hence we may assume that $B \in K$, so (3.1) becomes

$$A\zeta = A^\sigma \zeta^\sigma \qquad \text{for all } \sigma.$$

Let $\zeta_0$ be a given solution; dividing term by term we obtain $(\zeta/\zeta_0) = (\zeta/\zeta_0)^\sigma$ for all $\sigma$, whence $\zeta/\zeta_0 \in K$. However $K$ contains only finitely many roots of unity (in fact only $\pm 1$), as remarked above; this gives a contradiction.

(b) $L(\Gamma) \subset V := \{u + u^{-1} | u \in U\}$. Again, this implies, for some algebraic numbers $A, B$, $A \neq 0$, and infinitely many roots of unity $\zeta$, that $A(\zeta + \zeta^{-1}) + B \in K$.

We argue as before and conjugate by a $\sigma \in G_K$, obtaining

$$A\zeta + A\zeta^{-1} - A^\sigma \zeta^\sigma - A^\sigma \zeta^{-\sigma} + (B - B^\sigma) = 0. \tag{3.2}$$

Again, suppose first that $B \notin K$ and pick $\sigma$ so that $B \neq B^\sigma$. Now, (3.2) may not be normalized since there may be some vanishing subsum. We then consider a vanishing minimal subsum containing the term $B - B^\sigma$. This subsum may vary

with $\zeta$, but only in finitely many ways. In each case we obtain a finite number of solutions by [5], getting a contradiction. So we may assume as before that $B \in K$.

We multiply (3.2) by $\zeta$, obtaining for all $\sigma$

$$A + A\zeta^2 - A^\sigma \zeta^{1+\sigma} - A^\sigma \zeta^{1-\sigma} = 0. \tag{3.3}$$

The coefficients of the linear relation among roots of unity given by (3.3) involve only $A, A^\sigma$, hence we have only a finite number of possible coefficients in the relations for varying $\sigma$.

The *indecomposable* relations (i.e., those with no proper vanishing subsum) give rise by [4] only to finitely many roots of unity $\zeta$. Therefore we may assume that for each $\sigma$, (3.3) is decomposable. In turn there are three possibilities:

(bi) $1 + \zeta^2 = 0$: now there are at most two solutions.
(bii) $\zeta^{1+\sigma} = A^{1-\sigma}$ and $\zeta^{1+\sigma} = A^{\sigma-1}$, which implies in particular $A^2 = A^{2\sigma}$.
(biii) $\zeta^{1-\sigma} = A^{1-\sigma}$ and $\zeta^{1-\sigma} = A^{\sigma-1}$, which again implies $A^2 = A^{2\sigma}$.

In both (bii) and (biii), squaring both sides of the equation $A(\zeta + \zeta^{-1}) = A^\sigma(\zeta + \zeta^{-1})^\sigma$ we obtain (taking into account all $\sigma$) that $\zeta^2 + \zeta^{-2} \in K$, and that this holds for infinitely many roots of unity $\zeta$.

Hence $\zeta^2$ has degree $\leq 2$ over $K$ and, by standard theory of cyclotomic fields, this implies that $\xi = \xi_\zeta := \zeta^{24}$ is a root of unity of $p$-power order (and hence lies in $K'$), such that $\xi + \xi^{-1} = T_{12}(\zeta^2 + \zeta^{-2}) \in K$.

In particular, $\xi \in K'$ has degree $\leq 2$ over $K$; but $K'$ has odd degree $l$ over $K$, which implies that $\xi \in K$. However, as remarked at the beginning, the only roots of unity contained in $K$ are $\pm 1$, so $\xi$ has only finitely many possibilities and we have a contradiction. This proves part (i).

To prove part (ii), namely that $K'$ has not the Property (P) it suffices to note that any polynomial $f(x) = x^d$, $d \geq 2$, satisfies $f(\Gamma) = \Gamma$, where $\Gamma$ is the set of roots of unity of $p$-th power order, which is contained in $K'$.

Finally, we prove (iii), namely that $K$ has not the Property (N).

Let $T = Tr_K^{K'}$ be the trace and let $\sigma$ be a generator for $\mathrm{Gal}(K'/K)$. We first prove the following claim: *For every $\alpha \in \overline{\mathbb{Q}}$ the equation $\alpha = T(\zeta)$ has only finitely many solutions $\zeta$ which are roots of unity of $p$-th power order.*

In fact, an equation $T(\zeta) = T(\xi)$, where $\zeta, \xi$ are roots of unity of orders resp. $p^r, p^s$, $r < s$, amounts to the linear relation $\zeta + \zeta^\sigma + \ldots + \zeta^{\sigma^{l-1}} = \xi + \xi^\sigma + \ldots + \xi^{\sigma^{l-1}}$ among $2l$ roots of unity; the results of [5] (or even a simpler result by Mann quoted therein) immediately imply that this is impossible: in fact any vanishing subsum must have at least $p > 2l$ terms.

The claim now immediately implies that $K$ contains infinitely many elements of bounded height: it suffices to take the traces $T(\zeta_{p^n})$ for $n = 1, 2, \ldots$; since $\zeta$ is an algebraic integer, the height $h(T(\zeta))$ is plainly $\leq \log l$.

This concludes the proof of Theorem 3.3. ■

## References

[1] E. Bombieri, W. Gubler, *Heights in Diophantine Geometry*, Cambridge Univ. Press, 2006.

[2] M. Baker, R. Rumely, *Equidistribution of small points, rational dynamics, and potential theory*, *Ann. Inst. Fourier* **56** (2006), 625–688.

[3] E. Bombieri, U. Zannier, *A Note on heights in certain infinite extensions of* $\mathbb{Q}$, *Rend. Mat. Acc. Lincei* **12** (2001), no. 9, 5–14.

[4] R. Dvornicich, U. Zannier, *Cyclotomic Diophantine Problems (Hilbert irreducibility and invariant sets for polynomial maps)*, *Duke Math. J.* **139** (2007), 527–554.

[5] R. Dvornicich, U. Zannier, *On sums of roots of unity*, Monatsh. Math. **129** (2000), 97–108.

[6] J. Milnor, *Dynamics in One Complex Variable*, $3^{nd}$ ed., Annals of Mathematical Studies, Princeton University Press, 2006.

[7] W. Narkiewicz, On polynomial transformations, *Acta Arith* **7** (1961/1962), 241–249.

[8] W. Narkiewicz, *Polynomial mappings*, Springer-Verlag LNM **1600**, 1995.

**Addresses:** Roberto Dvornicich Università di Pisa Largo Pontecorvo, 5 56127 Pisa, Italy
Umberto Zannier Scuola Normale Superiore Piazza dei Cavalieri, 7 56126 Pisa, Italy
**E-mail:** dvornic@dm.unipi.it, u.zannier@sns.it
**Received:** 3 December 2007; **revised:** 8 January 2008