SOME FIELD THEORETIC PROPERTIES AND AN APPLICATION CONCERNING TRANSCENDENTAL NUMBERS

CHRISTIAN U. JENSEN AND DIEGO MARQUES

ABSTRACT. For a proper subfield K of $\overline{\mathbb{Q}}$ we show the existence of an algebraic number α such that no power α^n, $n \geq 1$, lies in K. As an application it is shown that these numbers (multiplied by convenient rational or Gaussian rational numbers) can be written in the form $P(T)^{Q(T)}$ for some transcendental numbers T where P and Q are arbitrarily prescribed non-constant rational functions over $\overline{\mathbb{Q}}$.

1. Introduction

The origin of this paper was a result concerning the transcendency of some numbers appearing in certain exponential equations. This lead to some purely field theoretic questions, which may be of some independent interest. The first of the results are easy consequences of the famous

Theorem 1. *[Artin-Schreier] (Cf. [4]) Let M be an algebraically closed field. If the characteristic of M is zero, any proper subfield F of M such that $[M : F]$ is finite, is real closed (i.e. F is not algebraically closed but $F(\sqrt{-1})$ is algebraically closed) and thus $[M : F] = 2$. If the characteristic of M is a prime number there is no proper subfield F of M for which $[M : F]$ is finite.*

Remark 1. *Artin-Schreier's theorem implies that the absolute Galois group of any non real closed field contains no automorphisms of finite order ($\neq 1$).*

In Section 2 we give some field theoretic results to be used in the final Section 3. This section first brings a brief historical survey of classical famous theorems concerning transcendental numbers and then - as an application of the results in Section 2 - we show the existence of algebraic numbers that can be written as powers of two transcendental numbers of a very special form.

2. Some field theoretic properties

We start with some consequences of the Theorem 1. Although we later in the applications shall only need fields of characteristic zero, for the sake of completeness we also consider the characteristic p case in the first three propositions.

Proposition 1. *Let M be an algebraically closed field and F a proper subfield which is not real closed. Then there exist elements in M of arbitrarily large degree with respect to F.*

2000 *Mathematics Subject Classification.* 12-xx; 11J81.

Key words and phrases. Artin-Schreier, Galois theory, Gelfond-Schneider, Transcendental numbers.

Proof. In the case where the characteristic of M (= the characteristic of F) is a prime number p we may assume that F is a perfect field. Indeed, if there were an element $a \in F$ such that a were not the p-th power of an element in F then the polynomials $x^{p^e} - a$ were irreducible in $F[x]$ for *every* natural number e. This would give rise to elements in M of arbitrary high degrees with respect to F.

By Theorem 1 M is an infinite algebraic extension of F. Hence there exists an infinite strictly increasing sequence of finite extensions contained in M

$$F \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_i \subsetneq M_{i+1} \subsetneq \dots$$

All these extensions are separable so if α_i is a primitive element for M_i/F the degree of α_i with respect to F tends to infinity as i tends to infinity. □

Since real closed fields necessarily have characteristic 0, Proposition 1 implies

Proposition 2. *Let F be an arbitrary field. If the characteristic of F is zero and there exists an irreducible polynomial in $F[x]$ of degree > 2, then there exist irreducible polynomials in $F[x]$ of arbitrarily large degrees.*

If the characteristic of F is a prime number and there exists an irreducible polynomial in $F[x]$ of degree > 1, then there exist irreducible polynomials in $F[x]$ of arbitrarily large degrees.

Proposition 3. *Let M be an algebraically closed field and F a proper subfield which is not real closed. Then M cannot be generated by adjoining to F all elements having degree (with respect to F) at most some fixed number n.*

Proof. We may obviously assume that M is an algebraic extension of F. The Galois closure of the field obtained by adjoining all elements of degree (w.r.t. F) at most n has a Galoisgroup which is a subgroup of a direct product of symmetric groups of degrees $\leq n$. This Galois closure cannot be M, since otherwise the absolute Galois group of F would contain an automorphism of finite order ($\neq 1$). This contradicts Theorem 1 (cf. Remark 1.) □

If $\mathcal{F}$ is a family of polynomials with coefficients in the field $\overline{\mathbb{Q}}$ of all algebraic numbers, by $\mathcal{R}_{\mathcal{F}}$ we mean the field obtained by adjoining to $\mathbb{Q}$ all the roots of the polynomials in $\mathcal{F}$.

Clearly Proposition 3 implies

Corollary 1. *Let $\mathcal{F}$ be a family of polynomials in $\overline{\mathbb{Q}}[x]$ for which there exists a natural number t such the polynomials in $\mathcal{F}$ have degreee $\leq t$ and all coefficients of the polynomials in $\mathcal{F}$ have degree (with respect to $\mathbb{Q}$) $\leq t$. Then $\mathbb{Q}(\mathcal{R}_{\mathcal{F}})$ is a proper subfield of the field $\overline{\mathbb{Q}}$ of all algebraic numbers.*

The next theorem will be proved in several steps.

Theorem 2. *For any proper subfield K of $\overline{\mathbb{Q}}$ there exists an algebraic number α such that α^n does not lie in K for any natural number n.*

Theorem 2 is an immediate consequence of the following Theorem 4, whose proof depends on

Lemma 1. *Let $\mathbb{Q}(\zeta_n)$ be the n-th cyclotomic field. There exists a number $\alpha \neq 0$ in $\mathbb{Q}(\zeta_n)$ such that for every automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, σ not the identity, the quotient $\sigma(\alpha)/\alpha$ is not a root of unity.*

Proof. (The following results from algebraic number theory can e.g. be found in [7].) There exist (infinitely many) prime numbers $p \equiv 1$ modulo n. In the ring of algebraic integers in $\mathbb{Q}(\zeta_n)$ any such prime p splits into $\varphi(n)(= [\mathbb{Q}(\zeta_n) : \mathbb{Q}])$ distinct prime ideals of degree one. If $\mathfrak{p}$ is such a prime ideal, then $\sigma(\mathfrak{p}) \neq \mathfrak{p}$ for every $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, σ not the identity. Let h be the class number of $\mathbb{Q}(\zeta_n)$, then $\mathfrak{p}^h$ is a principal ideal. If α is a generator of this ideal the conjugates of α, i.e. $\sigma(\alpha)$, σ running through $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, generate distinct ideals. Hence for every $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, σ not the identity, the quotient $\sigma(\alpha)/\alpha$ is not a unit (i.e. an invertible element in the ring of algebraic integers), in particular not a root of unity. □

Theorem 3. *Let K be a field of characteristic 0 and L/K any extension where $K \subsetneq L$. Then there exists an element α in L such that no power $\alpha^n, n \geq 1$, lies in K.*

Proof. The assertion is trivial if L is not algebraic over K. So it suffices to consider the case where L/K is a finite algebraic extension. We may obviously assume that K is maximal subfield of L, i.e. there is no field lying strictly between K and L. Furthermore we may assume that there exists an element $\beta \in L \setminus K$ for which β^n lies in K for some integer $n > 1$.

We now distinguish between two cases:

i) $L = K(\zeta)$ for some root of unity ζ.

ii) $L \neq K(\zeta)$ for every root of unity ζ.

ad i) By Lemma 1 there exists an element α in $\mathbb{Q}(\zeta)$ such that for every σ in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, σ not the identity, the quotient $\sigma(\alpha)/\alpha$ is not a root of unity. This implies that $\sigma(\alpha^n) \neq \alpha^n$ for every $n \geq 1$. Therefore no power α^n, $n \geq 1$, lies in any proper subfield of $\mathbb{Q}(\zeta)$. Clearly $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$ and hence $L = K(\alpha)$.

Since $K \cap \mathbb{Q}(\zeta)$ is a proper subfield of $\mathbb{Q}(\zeta)$ the element α constructed above has the property that no power α^n, $n \geq 1$, lies in K.

ad ii) By assumption there exists an element β in $L \setminus K$ such that β^n lies in K for some $n > 1$. We may assume that n is the smallest such number. The polynomial $f(x) := x^n - \beta^n$ is an irreducible polynomial in $K[x]$. Indeed, $f(x) = \prod_{j=0}^{n-1}[x - \beta\zeta_n^j]$, where ζ_n is a primitive n-th root of unity. If $f(x)$ were reducible in $K[x]$, there would be an integer t, $1 \leq t \leq n-1$, such that for some n-th root of unity ζ the product $\beta^t \cdot \zeta$ would belong to K. Hence $K(\beta^t) = K(\zeta)$. Since K is a maximal subfield of L and β^t is not in K, we would get $L = K(\beta^t) = K(\zeta)$. But this contradicts our assumption ii). Hence $f(x)$ is irreducible in $K[x]$ and thus the degree $[L : K]$ is n.

The above, in particular, shows that if some non-trivial power of an element $\gamma \in L \setminus K$ lies in K, then γ^n lies in K and n is the smallest natural number with this property.

We apply this to $\gamma := 1 + \beta$. No non-trivial power of γ lies in K. Otherwise, the above remark shows that γ^n would lie in K. But since β^n lies in K the equation

$$\gamma^n = (1+\beta)^n = 1 + \binom{n}{1}\beta + \cdots + \binom{n}{n-1}\beta^{n-1} + \beta^n$$

shows that β would be root of a non-zero polynomial in $K[x]$ of degree $n-1$, contradicting the fact that the degree of β with respect to K is n. Thus no power of γ lies in K.

The proof of Theorem 4 is now complete. □

From the above we deduce

Corollary 2. *If we view $\overline{\mathbb{Q}}$ as a subfield of the complex number field $\mathbb{C}$, the algebraic numbers α such that no power α^n, $n \geq 1$, lies in a prescribed fixed proper subfield K of $\overline{\mathbb{Q}}$ form a dense subset of $\mathbb{C}$ (equipped with the usual topology).*

Proof. We distinguish between two cases: Either $K \subseteq \mathbb{R}$ or $K \nsubseteq \mathbb{R}$.

If $K \subseteq \mathbb{R}$ then we notice that no power α^n, $n \geq 1$, of an integer $\alpha = a + b \cdot i$ in the Gaussian field $\mathbb{Q}(i)$ lies in K if for instance a is an odd rational integer and b is an even rational integer. (Just consider the prime factorization of α and notice that $K \cap \mathbb{Q}(i) = \mathbb{Q}$.) Multiplying all these numbers by rational numbers we get the desired subset of $\mathbb{C}$.

If $K \nsubseteq \mathbb{R}$ the numbers in K lie dense in $\mathbb{C}$. So if α is some algebraic number such that $\alpha^n \notin K$, $n \geq 1$, then the numbers $\alpha \cdot k$, k running through K, yield the desired subset of $\mathbb{C}$. □

An immediate consequence of the previous results is

Theorem 4. *Let n be a fixed natural number and $\mathcal{F}$ the family of all polynomials in $\mathbb{Q}[x]$ of degree $\leq n$. Then the algebraic numbers α such that no power α^n, $n \geq 1$, lies in $\mathbb{Q}(\mathcal{R}_{\mathcal{F}})$ form a dense subset of $\mathbb{C}$.*

Although not necessary for the following we point out another aspect of Theorem 2. Let $\overline{\mathbb{Q}}^*$ be the multiplicative group of the non-zero elements of $\overline{\mathbb{Q}}$ and for a proper subfield K of $\overline{\mathbb{Q}}$ let K^* be the multiplicative group of the non-zero elements in K. Clearly the quotient group $\overline{\mathbb{Q}}^*/K^*$ is a divisible abelian group. An additively written divisible abelian group is the direct sum of copies of $\mathbb{Q}$ and copies of $\mathbb{Z}(p^\infty)$, p being a prime and $\mathbb{Z}(p^\infty)$ the divisible (= injective) hull of the cyclic group C_p of order p. (See e.g. [1])

Theorem 1 states that for a proper subfield K of $\overline{\mathbb{Q}}$ the quotient $\overline{\mathbb{Q}}^*/K^*$ is not a torsion group, in particular the corresponding (additively written) divisible group contains at least one copy of $\mathbb{Q}$. A sharper result is the following

Theorem 5. *Let K be a proper subfield of $\overline{\mathbb{Q}}$. Then the torsion-free part of the divisible quotient group $\overline{\mathbb{Q}}^*/K$ is isomorphic to the direct sum of countable many copies of $\mathbb{Q}$. The torsion part of $\overline{\mathbb{Q}}^*/K$ is non-trivial, i.e. contains at least one copy of $\mathbb{Z}(p^\infty)$ for some prime number p.*

Proof. We first prove the assertion concerning the torsion-free part of $\overline{\mathbb{Q}}^*/K$.

We start by considering the case where K is real closed. For each prime number $p_j \equiv 1 \pmod 4$ let π_j be an irreducible factor of p_j in the Gaussian ring $\mathbb{Z}[1, i]$. Then no product of powers ($\neq 1$) of π_j's lies in $\mathbb{Q}$ and hence not in K since $K \cap \mathbb{Q}(i) = \mathbb{Q}$.

Next assume K is not real closed. Then $[\overline{\mathbb{Q}} : K]$ is infinite; hence there exists an infinite tower of fields $K \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots \subsetneq K_i \subsetneq K_{i+1} \subsetneq \cdots$, where each field is a finite Galois extension of the previous. By theorem 2 for each i there exists an element α_i in $K_{i+1} \setminus K_i$ such that no power ($\neq 1$) of α_i lies in K_i. Then no product of powers ($\neq 1$) of the elements $\alpha_i, i \in \mathbb{N}$, lies in K. Therefore the corresponding residue classes of the α's in $\overline{\mathbb{Q}}^*/K$ gives rise to a direct sum of countably many of copies of $\mathbb{Q}$.

Concerning the torsion part of $\overline{\mathbb{Q}}^*/K$ the assertion is obvious if some root of unity does not lie in K. Hence we may assume that all roots of unity belong to K. Since, in particular, K is not real closed, $\overline{\mathbb{Q}}/K$ is a proper infinite Galois extension. This implies that there is an automorphism $\sigma \in Gal(\overline{\mathbb{Q}}/K)$ of order p^∞, for some prime number p. Hence there is a Galois extension of K whose Galois group is the additive group of $\mathbb{Z}_p$ of p-adic integers (cf. [3]). In particular, there will be a cyclic extension L/K of degree p. This extension must be a Kummer extension $K(\sqrt[p]{\alpha})$ for some $\alpha \in K$. Thus $\overline{\mathbb{Q}}^*/K$ contains an element of order p and therefore a copy of $\mathbb{Z}(p^\infty)$. $\square$

3. Application to transcendental number theory

Before giving an application of the previous results to transcendental numbers we briefly recall some - by now classic - facts concerning transcendental number theory.

At the 1900 International Congress of Mathematicians in Paris, Hilbert proposed his famous list of 23 problems and the seventh of them asked about the arithmetic nature of the powers x^y, where both these numbers are algebraic. In 1934, Gelfond [2] and Schneider [9], independently, completely solved the problem

Theorem 6 (Gelfond-Schneider)**.** *Assume α and β are algebraic numbers, with $\alpha \neq 0$ or 1, and β irrational. Then α^β is transcendental.*

It follows that $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{3}}$ and i^i are transcendental numbers. As well as e^π, because $e^\pi = (-1)^{-i}$.

This theorem also classifies the arithmetic nature of powers of two algebraic numbers. However, there is no a similar result for powers x^y when at least one of x and y is transcendental (see Table 1). In light of Theorem 6 we might think that the power of two transcendental numbers is still transcendental, but this is not the case ($e^{\log 2} = 2$).

x	y	x^y	Arithmetic nature
2	$\log 3/\log 2$	3	Algebraic
2	$i\log 3/\log 2$	3^i	Transcendental
e^i	π	-1	Algebraic
e	π	e^π	Transcendental
$2^{\sqrt{2}}$	$\sqrt{2}$	4	Algebraic
$2^{\sqrt{2}}$	$i\sqrt{2}$	4^i	Transcendental

Table 1. Possibilities

The case $x = y$ seems to be more interesting: can the number T^T be algebraic for some transcendental T? Sondow and the second author [10] showed that the answer for this question is yes, actually they proved that

Proposition 4 (*Cf. Proposition 1 in* [10]). *Given $A \in [e^{-1/e}, \infty)$, let $T \in \mathbb{R}^+$ satisfy $T^T = A$. If either*
(i). *$A^n \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ for all $n \in \mathbb{N}$, or*
(ii). *$A \in \mathbb{Q} \setminus \{n^n : n \in \mathbb{N}\}$,*
then T is transcendental. In particular, $T \notin \overline{\mathbb{Q}}$ if $T^T \in \mathbb{Q} \cap (e^{-1/e}, 1)$.

However, for instance, they were not able to work on the existence of algebraic numbers which can be written if the form $T^{T^{2009}+T+1}$, with T transcendental. Now using some results from the previous section we were able to solve completely this kind of problem

Theorem 7. *For arbitrary non-constant rational functions $P(x), Q(x) \in \overline{\mathbb{Q}}(x)$ the set of algebraic numbers of the form $P(T)^{Q(T)}$ with T transcendental, is dense in some open subset of the complex plane.*

Proof. The set of complex numbers for which $P(x)$ or $Q(x)$ has a pole or zero or $P(x)$ takes the value 1 is finite. The complement of this set inside $\mathbb{C}$ is an open subset of the complex plane. Let Ω be an open simply connected subset of the above open set. Choosing, for instance, the principal branch of the multi-valued logarithm function, the function $f(x) := P(x)^{Q(x)}$ is well defined and analytical in Ω. This function is a non-constant function. Indeed, since $P(x)$ and $Q(x)$ are non-constant and the algebraic numbers form a dense subset of $\mathbb{C}$ there exists an algebraic number β in Ω for which $Q'(\beta)P(\beta) \neq 0$. If $f(x)$ were constant then log $P(x) = -Q(x)P'(x)/Q'(x)P(x)$. Setting $x = \beta$ we get that log $P(\beta)$ would be an algebraic number. But this would contradict the famous theorem by Lindemann (cf [6]) that $\log \beta \notin \overline{\mathbb{Q}}$ for all $\beta \in \overline{\mathbb{Q}} \setminus \{0, 1\}$. Since a non-constant analytic function maps an open connected set of $\mathbb{C}$ onto an open connected set of $\mathbb{C}$ we see that $f(\Omega)$ is an open connected subset of $\mathbb{C}$.

Write $Q(x)$ as $Q_1(x)/Q_2(x)$, where $Q_1(x)$ and $Q_2(x)$ are polynomials in $\overline{\mathbb{Q}}[x]$. Let $\mathcal{F}$ be the family of polynomials of the form $Q_1(x) - dQ_2(x)$, d running through $\mathbb{Q}$. Clearly there exists an integer t such that every polynomial in $\mathcal{F}$ has degree $\leq t$ and all coefficients of these polynomials have a degree (with respect to $\mathbb{Q}$) $\leq t$.

Hence Corollary 1 implies that $\mathbb{Q}(\mathcal{R}_{\mathcal{F}}) \neq \overline{\mathbb{Q}}$. By Corollary 2 the algebraic numbers α such that no power α^n, $n \geq 1$ lies in $\mathbb{Q}(\mathcal{R}_{\mathcal{F}})$ form a dense subset of $\mathbb{C}$. Since $f(\Omega)$ is open, it contains dense subset of numbers α with the above property. Every α in this dense set has the form $\alpha = f(T) = P(T)^{Q(T)}$. This number T must be transcendental. In fact, assume T were algebraic. Since $P(T) \notin \{0, 1\}$ by the Gelfond-Schneider theorem we conclude that $Q(T)$ would be a rational number say $d = \frac{r}{s}$, r and s integers and $s > 0$. Hence T would belong to $\mathcal{R}_{Q_1(x) - \frac{r}{s}Q_2(x)} \subseteq \mathcal{R}_{\mathcal{F}}$. But then $\alpha^s = P(T)^r$ and thus $\alpha^s \in \mathbb{Q}(\mathcal{R}_{\mathcal{F}})$ contradicting the choice of α. $\square$

Remark 2. *Note that for any transcendental number T and any non-constant rational function $P \in \overline{\mathbb{Q}}(x)$, the number $P(T)$ is transcendental. On the contrary, the number T would be a root of the algebraic polynomial $P_1(x) - AP_2(x)$ (setting $P = P_1/P_2$), however all the roots of a such polynomial are algebraic by the algebraic closeness of $\overline{\mathbb{Q}}$.*

Example 1. *If $P(x) = x$ and $Q(x) = x^2$, then easy calculations show that the set of the algebraic numbers in the form T^{T^2}, with T transcendental, is dense in the interval $[1/\sqrt{e}, +\infty)$.*

In light of what we just proved, the following problem arises: is there algebraic number in the form T^{T^T}, for some transcendental T? And in the form $T^{T^{T^T}}$? And so on?

This question is still open. We recall the main open problem in transcendental theory which is the well-known Schanuel's conjecture (see [5] for its statement). In his Ph.D thesis [8, p. 32], the second author proved that

Proposition 5. *Suppose that Schanuel's conjecture is true. For any $m \geq 3$ and any algebraic number $1 \leq A \notin \mathbb{N}$, there exists a transcendental number T such that* $A = \underbrace{T^{T^{\cdot^{\cdot^{\cdot^{T}}}}}}_{m}$.

We finish by a related question which may be considered as an inverse problem of Theorem 7.

Question 1. *Give example, if any, of a well-known transcendental number T (like $e, \pi, \log 2$, etc) such that there exist non-constant rational functions $P(T), Q(T) \in \overline{\mathbb{Q}}(x)$, such that $P(T)^{Q(T)}$ is algebraic.*

In thus connection, the second author has proved, in a paper in preparation, that if Schanuel's conjecture is true then $P(e)^{Q(e)}$ is transcendental, for any non-constant rational functions $P(T), Q(T) \in \overline{\mathbb{Q}}(x)$.

Acknowledgement

References

1. L. Fuchs, *Infinite abelian Groups* Vol. I, Academic Press, New York-London, 1970.
2. A. O. Gelfond, *Sur le septième problème de Hilbert*, Investia Akad. Nauk. **7** (1934), 623-630.
3. Wulf-Dieter Geyer, *Unendliche algebraische Zahlkörper über denen jede Gleichung auflösbar von beschränkter Stufe ist.* J. Number Theory (1969) **1** , 346-374.
4. N. Jacobson, *Basic Algebra* II, (2-nd edition), W.H.Freeman, New York, 1989.
5. S. Lang, *Introduction to Transcendental Numbers,* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966
6. F. Lindemann, *Über die zahl* π, Math. Annalen **20** (1882) 213-225.
7. D. A. Marcus, *Number Fields*, Springer Verlag, New York Ind., 1977
8. D. Marques, *O problema de Lang e uma generalização dos teoremas de Stäckel*, Ph.D thesis, Universidade de Brasília, 2009.
9. T. Schneider, *Transzendenzuntersuchungen periodischer funktionen: I transzendenz von potenzen; II transzendenzeigenschaften elliptischer funktionen*, J. Reine Angew. Math. **172** (1934), 65-74.
10. J. Sondow, D. Marques, *Algebraic and transcendental solutions of some exponential equations*, 2009 (submitted).

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF COPENHAGEN, COPENHAGEN, DENMARK

E-mail address: `cujensen@math.ku.dk`

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDADE DE BRASÍLIA, BRASÍLIA, DF, BRAZIL

E-mail address: `diego@mat.unb.br`