FUNDAMENTA
MATHEMATICAE
207 (2010)

Schanuel Nullstellensatz for Zilber fields

by

P. D'Aquino (Napoli), **A. Macintyre** (London) and **G. Terzo** (Napoli)

Abstract. We characterize the unsolvable exponential polynomials over the exponential fields introduced by Zilber, and deduce Picard's Little Theorem for such fields.

1. Introduction. In this paper we work with the class of exponentially-algebraically closed exponential fields introduced by Zilber in [24]. For the subclass of Zilber fields which are strongly closed and have the countable closure condition he establishes categoricity in each uncountable power, and puts forward the dramatic conjecture that the classical complex exponential field is the unique model of power continuum. The huge importance of this conjecture for the classical case is that Zilber has, unconditionally, established, for the Zilber fields, geometrically natural criteria for solvability of systems of exponential equations, whereas in the classical case only a very few such criteria have been established (and then by using hard complex analysis, for example Nevanlinna Theory).

There is one beautiful result which has been proved analytically for the complex case, but which is far from obvious for Zilber fields. This is what we call the Schanuel Nullstellensatz (SN), which was conjectured by Schanuel (but it is not directly connected to Schanuel's famous Conjecture, also prominent in the Zilber case). For the complex field, it was proved by Henson and Rubel [5] using very serious Nevanlinna Theory. The main result of our paper is that it also holds for the Zilber fields. We give the exact statement later, once we have established some formalism. But the reader will get the flavour if we express it as "An exponential polynomial has no zero iff it is the exponential of another exponential polynomial". From (SN) we will deduce a version of Picard's Little Theorem for Zilber fields purely algebraically (it could not be otherwise, since Zilber's Conjecture implies that the complex topology is not

2010 *Mathematics Subject Classification*: 03Cxx, 03C60.
Key words and phrases: exponential field, Schanuel's Conjecture, strong extension.

DOI: 10.4064/fm207-2-2

first-order definable from the basic operations of the complex exponential field).

2. Zilber fields. An *exponential field*, or for short an *E-field*, is a pair (K, E) where K is a field and E is a morphism from the additive group structure of K to the multiplicative group of K, that is, $E(x+y) = E(x)E(y)$ for all $x, y \in K$. If E is only partially defined we refer to (K, E) as a *partial exponential structure*.

The class of E-fields has been studied for the last 35 years, originally motivated by understanding the elementary theory of the real exponential field [13], [3]. The main results concerning the real exponential field go back to the early nineties with the work of A. Wilkie.

Schanuel's Conjecture has already played a crucial role in the real case, giving the decidability of the theory of the real exponential field, as shown by Macintyre and Wilkie [14]. The complex exponential field is unconditionally undecidable, but this does not, as Zilber saw, stand in the way of a deep model-theoretic analysis.

Zilber saw a subtle connection between Schanuel's Conjecture (SC) and the technology of predimensions introduced by Hrushovski [7]. Quite independent of the truth of (SC) for the complex exponential field, there are exponential fields [24] in which (SC) holds, and in which the periods of exponentiation form an infinite cyclic group. This has been known for a long time. The great novelty is to observe that if we consider the Hrushovski predimension corresponding to (SC) (see below) and work in the category of exponential fields satisfying (SC) with the corresponding notion of strong embedding, then there are existentially closed structures, which can be characterized by geometrically natural axioms for solvability of exponential systems. Among the existentially closed structures are the strong existentially closed structures, characterized by having "generic" solutions for the systems in the axioms and a countable closure, and it is for these that Zilber shows uncountable categoricity. For the details, see [24].

Everything we do depends on [24], though the formalism is not always to our taste. Zilber works in an unusual language $\mathcal{L}$ containing $+$, n-ary predicate symbols V for $V \subseteq F^n$ an affine algebraic variety defined and irreducible over $\mathbb{Q}$, unary function symbols $\frac{1}{m}\cdot$ for each integer $m > 0$, and a binary relation $E(x, y)$. Let $\mathcal{L} = \mathcal{L}^- \cup \{E\}$. There is thus a forced notion of structure and substructure for this mixed functional-relational formalism.

This formalism is suitable for dealing with substructures of exponential fields of characteristic 0 (for the basic definitions about exponential fields, see [13], [12]). E corresponds to the graph of exponentiation, and may be partial

in a substructure, if one works, as Zilber does, in a formalism involving relations. $\frac{1}{m}\cdot$ stands for multiplication by $\frac{1}{m}$, $+$ for addition, V for $V \subseteq F^n$, where F is the ambient field. Obviously the graph of multiplication can be defined in terms of the variety corresponding to its graph. $E(F)$ will denote the set $\{y : \exists x \in F \text{ such that } E(x, y)\}$.

Zilber identifies the basic class $\mathcal{E}$ of $\mathcal{L}$-structures F which are algebraically closed fields of characteristic 0, where the symbols of the language have their natural interpretations and E is the graph of a surjective homomorphism

$$\mathrm{ex} : (F, +) \to (F^*, \cdot)$$

(as it is in the case of $\mathbb{C}$).

An $\mathcal{L}$-structure $\mathcal{A}$ belongs to the class $sub\mathcal{E}$ if there is an $\mathcal{L}$-structure F such that $\mathcal{A} \subseteq F$ as $\mathcal{L}^-$-structures, $E^{\mathcal{A}} \subseteq E^F$, and the domain of exponentiation on $\mathcal{A}$ is a $\mathbb{Q}$-vector space, under the natural operations.

$sub\mathcal{E}_{\mathrm{st}}$ denotes the class of those structures $\mathcal{A}$ in $sub\mathcal{E}$ having *standard full kernel*, i.e. $\ker(\mathrm{ex}) = \{a \in \mathcal{A} : \mathrm{ex}(a) = 1\} = \omega\mathbb{Z}$, where ω is in $\mathcal{A}$ and is transcendental over $\mathbb{Q}$.

Zilber has a more elaborate definition of this notion, but in fact his extra conditions are redundant. In what follows, we will refer to the elements of the kernel of exponentiation also as *periods*.

An example of a structure belonging to $sub\mathcal{E}_{st}$ is $\mathcal{A} = \mathbb{C}$, where $\omega = 2i\pi$ and domain of exponentiation $D_{\mathcal{A}} = \mathbb{Q}\omega$, and $\mathrm{ex} = \exp|_{D_{\mathcal{A}}}$.

Crucial to Zilber's model theory of exponentiation is the condition SC (Schanuel's Conjecture)

Schanuel's Conjecture (SC). Let $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, E(\lambda_1), \ldots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$.

In a straightforward way Schanuel's Conjecture can be formulated for any exponential structure of characteristic 0.

In his paper Zilber uses the notion of strong extension (inspired by Hrushovski's work [7]) in order to define the class of existentially strongly closed structures in the class of exponential fields of characteristic 0 satisfying Schanuel's Conjecture, and with full standard kernel.

2.1. Strong extensions. Let $\mathcal{S}$ be an $\mathcal{L}$-structure. We denote the domain of exponentiation in $\mathcal{S}$ by $D_{\mathcal{S}}$. If $A \subset \mathcal{S}$ then $\langle A \rangle_{\mathbb{Q}}$ is the $\mathbb{Q}$-vector space generated by A.

Definition 2.1. Let A be a finite subset of $D_{\mathcal{S}}$. We define the *predimension* of A as

$$\delta_{\mathcal{S}}(A) = \text{t.d.}(A \cup E(\langle A\rangle_{\mathbb{Q}})) - \text{l.d.}(A)$$

where t.d.(A) is the transcendence degree of A over $\mathbb{Q}$ and l.d.(A) is the linear dimension of A over $\mathbb{Q}$.

Note that the predimension of A is the same as the predimension of $\langle A\rangle_{\mathbb{Q}}$.

Since we are working with structures which satisfy Schanuel's Conjecture we will always have $\delta_{\mathcal{S}}(A) \geq 0$ for all finite $A \subseteq D_{\mathcal{S}}$. (This is actually an equivalent form of Schanuel's Conjecture.)

$sub\mathcal{E}^0$ denotes the class of structures $\mathcal{R} \in sub\mathcal{E}$ such that $\delta_{\mathcal{R}}(A) \geq 0$ for all finite $A \subseteq D_{\mathcal{R}}$, and $\mathcal{E}^0 = \mathcal{E} \cap sub\mathcal{E}^0$.

Some care is needed when we work with structures where exponentiation is only a partial function. If $\mathcal{R}, \mathcal{S}$ are structures on which only a partial exponential function is defined, then for some finite $A \subset \mathcal{R}$ it can happen that $\delta_{\mathcal{R}}(A) < \delta_{\mathcal{S}}(A)$. This happens since some elements of A may not have exponentials in $\mathcal{R}$ but they have exponentials in $\mathcal{S}$. So in $\mathcal{S}$ there is extra transcendence degree. This problem does not exist when exponentiation is total.

We let $\delta_{\mathcal{R}}(B/A) = \delta_{\mathcal{R}}(B \cup A) - \delta_{\mathcal{R}}(A)$ when A and B are finite subsets of $\mathcal{R}$, but we need to extend this notion to the case of general A. Here we use an inductive procedure very common in geometric model theory.

Definition 2.2. Let B be a finite subset of $\mathcal{R}$ and A an infinite subset of $\mathcal{R}$. For any integer k we define $\delta_{\mathcal{R}}(B/A) \geq k$ to mean that for each finite subset W of A there is a finite subset W' of A, extending W, such that $\delta_{\mathcal{R}}(B/W') \geq k$. Then $\delta_{\mathcal{R}}(B/A) = k$ means that $\delta_{\mathcal{R}}(B/A) \geq k$ but not $\delta_{\mathcal{R}}(B/A) \geq k+1$.

Definition 2.3. Let $\mathcal{R}, \mathcal{S} \in sub\mathcal{E}$. Then $\mathcal{S}$ is a *strong extension* of $\mathcal{R}$ (written $\mathcal{R} \leq \mathcal{S}$) if $\mathcal{R} \subseteq \mathcal{S}$ and the following two conditions hold:

(i) $\delta_{\mathcal{R}}(A/B) \leq \delta_{\mathcal{S}}(A/B)$ for any finite subsets A, B of $\mathcal{R}$.
(ii) $\delta_{\mathcal{S}}(B/D_{\mathcal{R}}) \geq 0$ for any $B \subset_{\text{fin}} D_{\mathcal{S}}$.

Remark 2.4. Condition (i) is always satisfied if the exponential function over A is total, but we do need to use it in other cases, too.

Let $\mathcal{R} \in sub\mathcal{E}^0$. For any finite $A \subset \mathcal{R}$ the *dimension* of A in $\mathcal{R}$ is

$$\dim_{\mathcal{R}}(A) = \min\{\delta_{\mathcal{R}}(B) : A \subseteq B \subset_{\text{fin}} D_{\mathcal{R}}\}.$$

If $\mathcal{R}$ and $\mathcal{S}$ are exponential structures where exponentiation is total and satisfy Schanuel's Conjecture then

$$\mathcal{R} \leq \mathcal{S} \quad \text{iff} \quad \dim_{\mathcal{R}}(A) = \dim_{\mathcal{S}}(A) \text{ for all } A \subseteq_{\text{fin}} \mathcal{R}.$$

We recall the following properties of strong extensions proved in [24, p. 71].

LEMMA 2.5.

(i) *If* $\mathcal{R} \leq \mathcal{S}$ *and* $\mathcal{S} \leq \mathcal{Z}$, *then* $\mathcal{R} \leq \mathcal{Z}$.
(ii) *If* $(I, <)$ *is a chain and* $\mathcal{R}_i \leq \mathcal{R}_j$ *for* $i \leq j$, *then* $\mathcal{R}_i \leq \bigcup_{i \in I} \mathcal{R}_i$ *for all* $i \in I$.

Zilber also shows that a structure with partial exponentiation satisfying Schanuel's Conjecture can always be extended by a strong embedding to a structure with total exponentiation preserving periods and still satisfying Schanuel's Conjecture (see [24, Lemma 2.11, p. 73]).

LEMMA 2.6. *Let* $\mathcal{R} \in sub\mathcal{E}^0$ *with full kernel. Then there is* $F \in \mathcal{E}^0$ *and an embedding of* $\mathcal{R}$ *into* F *such that* $\mathcal{R} \leq F$ *and* $\ker|_F = \ker|_{\mathcal{R}}$.

The proof of our main result (see Theorem 4.6) will consist in the construction of a strong extension of a certain exponential structure. Right now, we provide an example of a very natural extension of an exponential field which is not a strong extension.

THEOREM 2.7. $(\mathbb{C}, e^x)$ *is not a strong extension of* $(\mathbb{R}, e^x)$ *assuming* (SC).

Proof. First note that

$$\delta_{\mathbb{R}}(\pi) = \text{t.d.}(\pi, e^{\pi}) - \text{l.d.}(\pi) = 1 \tag{1}$$

by Nesterenko's great theorem [17] (although we may as well use (SC), as we use it below). And again by Nesterenko's result,

$$\delta_{\mathbb{C}}(\pi, i\pi) = \text{t.d.}(\pi, i\pi, e^{\pi}, e^{i\pi}) - \text{l.d.}(\pi, i\pi) = 0. \tag{2}$$

Notice that (1) and (2) have been obtained unconditionally. By (SC) the dimension of π in $\mathbb{C}$ is 0. If the extension is strong then there must be a finite subset B of $\mathbb{R}$, $\mathbb{Q}$-linearly independent over π, so that the predimension of $B \cup \{\pi\}$ is 0. But B, π and $i\pi$ are linearly independent over $\mathbb{Q}$, and so the predimension of $B \cup \{\pi, i\pi\}$ in $\mathbb{C}$ is -1, contradicting (SC). ∎

The refereee pointed out to us the example in Kirby [8] showing unconditionally that $(\mathbb{C}, e^x)$ is not a strong extension of $(\mathbb{R}, e^x)$. This is short and easy, using the first definition of strong extension. We prefer to keep our example as it is more explicit about the dimension of π, which is of basic importance. Note that Macintyre and Wilkie showed that Schanuel's Conjecture implies that π is not in the prime model of $(\mathbb{R}, e^x)$ [14].

2.2. Exponentially-algebraically closed structures. We now identify those exponential fields F in $\mathcal{E}^0_{\text{st}}$ (i.e. those structures of $\mathcal{E}$ which have standard full kernels and satisfy Schanuel's Conjecture) in which there are solutions of as many equations as possible without violating Schanuel's Conjecture or adding new periods, or lowering a predimension.

Let $G_n(F) = F^n \times (F^*)^n$, the F-points of an algebraic group over $\mathbb{Q}$.

DEFINITION 2.8. A structure F in $\mathcal{E}^0_{\rm st}$ is said to be *exponentially-algebraically closed* if whenever $W \subset V \subseteq G_n(F)$ are irreducible varieties defined over F and there are $K \in \mathcal{E}^0_{\rm st}$ and $\overline{a} \in K^n$ such that $F \leq K$ and $(\overline{a}, \exp(\overline{a})) \in V - W$, then there is $\overline{c} \in F^n$ such that $(\overline{c}, \exp(\overline{c})) \in V - W$.

It is clear (and proved in [24]) that F is algebraically closed. As Zilber remarks, K does not need to range over $\mathcal{E}^0_{\rm st}$ but it is enough to consider partial exponential structures thanks to Lemma 2.6. This observation will be crucial in the proof of our main result.

The class of exponentially-algebraically closed structures in $\mathcal{E}^0_{\rm st}$ is denoted by $\mathcal{EC}_{\rm st}$. In [24] the author proves that the class $\mathcal{EC}_{\rm st}$ has an $\mathcal{L}_{\omega_1\omega}$-axiomatization. He uses some conditions on varieties which are $\mathcal{L}_{\omega_1\omega}$-definable. Moreover, Schanuel's Conjecture and having full standard kernel are $\mathcal{L}_{\omega_1\omega}$-definable properties. We briefly review the axiomatization. Let $T = (a_{ij})$ be a $k \times n$ matrix of integers and

$$[T] : G_n(F) \to G_k(F)$$

be the homomorphism given by

$$\langle z_1, \ldots, z_n, w_1, \ldots, w_n \rangle \mapsto \langle z'_1, \ldots, z'_k, w'_1, \ldots, w'_k \rangle$$

where

$$z'_i = a_{i1}z_1 + \cdots + a_{in}z_n \quad \text{and} \quad w'_i = w_1^{a_{i1}} \cdots w_n^{a_{in}}$$

for $i = 1, \ldots, k$.

DEFINITION 2.9. The variety $V \subseteq G_n(F)$ is *normal* if $\dim_F V' \geq k$, where $V' = [T](V)$ for any $k \times n$ matrix of integers T of rank k where $1 \leq k \leq n$.

DEFINITION 2.10. The variety $V \subseteq G_n(F)$ is *free* if we cannot find $a_1, \ldots, a_n \in \mathbb{Z}$ and $b, d \in K$ with $d \neq 0$ such that V is contained in either variety

$$\{(\overline{z}, \overline{w}) : a_1z_1 + \cdots + a_nz_n = b\} \quad \text{or} \quad \{(\overline{z}, \overline{w}) : w_1^{a_1} \cdots w_n^{a_n} = d\}.$$

REMARK 2.11. The conditions of normality and freeness for a variety avoid the existence of any further algebraic relation among the coordinates of a point in the variety (except those imposed by the variety itself) which could be an obstruction for intersecting the graph of exponentiation.

The condition of normality can be expressed equivalently by saying that for all generic points of V' the following inequality holds:

$$\text{t.d.}\, \mathbb{Q}(z'_1, \ldots, z'_k, w'_1, \ldots, w'_k) \geq k.$$

Part of [24] is devoted to showing that the properties of normality and freeness are first order definable.

We will call the exponentially-algebraically closed fields *Zilber fields*. The $\mathcal{L}_{\omega_1\omega}$-axiomatization of the class of Zilber fields is given by the following characterization (see Proposition 4.3 of [24]).

THEOREM 2.12. *Let $F \in \mathcal{E}^0_{\mathrm{st}}$. Then F is exponentially-algebraically closed iff for every variety $V \subseteq G_n(F)$ defined over F that is irreducible, normal and free there is $\overline{a} \in F^n$ such that $(\overline{a}, E(\overline{a})) \in V$.*

The above theorem implies that in a Zilber field we can solve certain systems of polynomial equations. Zilber goes on to add conditions guaranteeing categoricity in uncountable cardinalities.

Zilber obtains a remarkable categoricity result for the class of exponentially-algebraically closed fields satisfying a countable closure condition and a weak saturation property (for details see [24]).

3. E-polynomial ring. For any exponential field (or E-field) (K, E) we can construct the ring of exponential polynomials over K. We use it now when K is a Zilber field. For the proof of our main result it is useful to review the construction of the E-polynomial ring, and related notions of exponential algebra (see also [3]).

Let (K, E) be an E-field. The ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$ is an E-ring constructed in the following way by recursion. We construct three sequences:

1. $(R_k, +, \cdot)_{k \geq -1}$ are rings;
2. $(B_k, +)_{k \geq 0}$ are torsion free abelian groups, and in the case of Zilber's fields, the elements of the sequence are also divisible groups;
3. $(E_k)_{k \geq -1}$ are partial E-morphisms.

STEP 0. We define $R_{-1} = K$; $R_0 = (K[\overline{X}], +, \cdot)$; B_0 is the ideal generated by $\overline{X}$, $R_0 = R_{-1} \oplus B_0$ and $E_{-1} : R_{-1} \to R_0$, is the composition of the initial E-morphism over K with the immersion of K into $K[\overline{X}]$.

INDUCTIVE STEP. Suppose that $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that

$$R_k = R_{k-1} \oplus B_k, \qquad E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot),$$

where $\mathcal{U}(R_k)$ denotes the set of units in R_k. Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

be a formal isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \quad \text{(as group ring over } R_k).$$

Therefore R_k is a subring of R_{k+1}, and as additive group

$$R_{k+1} = R_k \oplus B_{k+1},$$

where B_{k+1} is the R_k-submodule of R_{k+1} freely generated by t^b, with $b \in B_k$ and $b \neq 0$ (this last condition ensures that B_{k+1} does not coincide with R_{k+1}). We define $E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot)$ as follows:

$$E_k(x) = E_{k-1}(r) \cdot t^b \quad \text{for } x = r + b,\ r \in R_{k-1} \text{ and } b \in B_k.$$

In this way we construct a chain of partial E-rings (the domain of exponentiation of R_{k+1} is R_k) $R_0 \subset R_1 \subset \cdots$. Then the *E-polynomial ring* is

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k$$

and the E-ring morphism defined on $K[\overline{X}]$ is the following:

$$E(x) = E_k(x) \quad \text{if } x \in R_k,\ k \in \mathbb{N}.$$

Notice that each R_{k+1} as additive group is the direct sum $K \oplus B_0 \oplus B_1 \oplus \cdots \oplus B_{k+1}$. Moreover, as an additive group, $K[X_1, \ldots, X_n]^E$ can be considered as $K \oplus B_0 \oplus B_1 \oplus \cdots$.

Recall that for all k the group ring R_{k+1} can be viewed in the following different ways:

$$R_{k+1} \cong R_0[t^{B_0 \oplus \cdots \oplus B_k}]; \quad R_{k+1} \cong R_1[t^{B_1 \oplus \cdots \oplus B_k}]; \quad \ldots \quad R_{k+1} \cong R_k[t^{B_k}].$$

Moreover, $K[X_1, \ldots, X_n]^E = R_0[t^{B_0 \oplus B_1 \oplus \cdots}]$, i.e. $K[X_1, \ldots, X_n]^E$ is a group ring constructed over a UFD $U = K[X_1, \ldots, X_n]$ $(= R_0)$ and a torsion free divisible abelian group $G = t^{B_0 \oplus B_1 \oplus \cdots}$ (a $\mathbb{Q}$-vector space).

Remark 3.1. From the construction of $K[\overline{X}]^E$, for any exponential polynomial $f(\overline{X})$ there is $k \in \mathbb{N}$ such that $f(\overline{X}) \in R_{k+1} - R_k$, where $R_{k+1} = R_k[t^{B_k}]$. Following [3] we will refer to $k+1$ as the *height* of f.

Recalling that t^{B_k} is freely generated by t^{b_j} for $b_j \in B_k$, modulo the exponential identities, we can write $f(\overline{X})$ uniquely as

$$f(\overline{X}) = \sum_{h=1}^{m} a_h t^{b_h},$$

where $a_h \in R_k$ and $b_h \in B_k$. We observe that $t^{b_1}, \ldots, t^{b_m}$ are linearly independent over R_k.

However, for what follows, the representation of $K[\overline{X}]^E$ as a group ring over U $(= R_0)$ is more important. That is, $f(\overline{X})$ can be written uniquely as

$$f(\overline{X}) = \sum_{h=1}^{m} a_h t^{b_h},$$

where $a_h \in R_0$ and $b_h \in B_1 \oplus B_2 \oplus \cdots$.

We recall the following characterization of the invertible elements in any E-polynomial ring (see [3]).

PROPOSITION 3.2. *If R is an integral domain of characteristic 0, then $R[\overline{X}]^E$ is an integral domain whose units are of the form $u \cdot E(p)$, where u is a unit of R and $p \in R[\overline{X}]^E$.*

This is in fact a special case of a standard theorem about units of group rings of torsion-free abelian groups over domains of characteristic zero [10], since $K[\overline{X}]^E$ is such a group ring. We study divisibility in $K[\overline{X}]^E$ via divisibility in the group ring over the polynomial ring U. Irreducibility is of course the first notion to consider, and to work with that we need to know the units. Recall that an *associate* of an element is any product of it by a unit, and that an element is *irreducible* if its only divisors are associates.

The main point is that the units of $R[G]$, when R is a characteristic zero domain, and G is a torsion-free abelian group, are the elements of the form ut^g where u is a unit of R, and $g \in G$. In the special case when R is the above U, the units of R are exactly the nonzero elements of K.

REMARK 3.3. From the construction of $K[\overline{X}]^E$ it follows that for each k, R_{k+1} is a strong extension of R_k. Conditions (i) and (ii) of Definition 2.3 are satisfied since at each step of the construction the new exponentials are added as freely as possible over the elements in the previous ring. Moreover, the domain of exponentiation of each R_k is a $\mathbb{Q}$-vector space. By Lemma 2.5, $K[\overline{X}]^E$ is a strong extension of K.

From (ii) of Definition 2.3 it also follows that if K satisfies Schanuel's Conjecture, so do all the R_k's, and hence also $K[\overline{X}]^E$.

We notice that at each step in the construction no new periods have been introduced. So, $\ker(E_K) = \ker(E_{K[\overline{X}]^E})$.

3.1. A factorization theorem. In the literature on exponential algebra there is no detailed account of a theory of factorization for exponential polynomials. There are, however, a few important papers, of which we were unaware until fairly recently ([20], [4], [11], [18], [19]). It seems that Ritt and Gourin were the first to consider a factorization theory for exponential polynomials over an algebraically closed field K of characteristic 0, and with only one iteration of exponentiation. They worked with the group ring $U[G]$, where $U = K[x]$ and G is the group of pure exponential terms. They reduce the study of factorization in $U[G]$ to that of $U[y_1, \ldots, y_k]$ (k varying), and to polynomials $f(y_1^{\mu_1}, \ldots, y_k^{\mu_k})$ with $\mu_1, \ldots, \mu_k \in \mathbb{N}_+$. We will adapt their results to our setting, i.e. the group ring $U[G]$ is constructed over the unique factorization domain $U = K[\overline{X}]$ and the group G is $t^{B_1 \oplus B_2 \oplus \cdots}$.

The basic idea is to attach to elements f of $U[G]$ polynomials over U in fractional powers of many variables. For our purposes there is no need to be canonical. Here is the basic idea.

As observed before, an exponential polynomial $f(\overline{X})$ can be written uniquely as

$$f(\overline{X}) = \sum_{h=1}^{m} a_h t^{b_h},$$

where $a_h \in R_0 = K[\overline{X}]$ and $b_h \in B_1 \oplus B_2 \oplus \cdots$.

Let Γ be the abelian additive group generated by $b_1, \ldots, b_m$. The $\mathbb{Q}$-space generated by Γ is denoted by $\mathrm{supp}(f)$, the *support* of f. Choose a $\mathbb{Z}$-base $\{\beta_1, \ldots, \beta_l\}$ of Γ. This choice is noncanonical, but we ignore this point. Without loss of generality we can consider f as a polynomial in $t^{\beta_1}, \ldots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$.

We use formally $\omega_1, \ldots, \omega_l$ for $t^{\beta_1}, \ldots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \ldots, \omega_l]$. Later we will refer to the *associate polynomial* of f. Notice that there is no connection with the notion of associate connected with divisibility, which we will also use.

Suppose f is irreducible in $K[\overline{X}]^E$. Then, clearly, f is irreducible in $R_k[\omega_1, \ldots, \omega_l]$. It is much less obvious, but true, that f is also prime in $R_k[\omega_1, \ldots, \omega_l]$. This follows from the work of Ritt and his followers, which we now review.

One of Ritt's most fundamental results is that if f factors as $f_1 f_2$ then $\mathrm{supp}(f_i) \subseteq \mathrm{supp}(f)$ for $i = 1, 2$, up to associates (i.e. up to multiplying by units of $K[\overline{X}]^E$). If we translate this into a formulation involving the polynomials over U associated to the f_i's, then we are led to issues about factoring polynomials into polynomials in fractional powers, the main concern of the literature cited earlier.

We need some definitions. Let $\overline{x} = (x_1, \ldots, x_n)$. By a *monomial* in the variables $x_1, \ldots, x_n$ we mean $x_1^{m_1} \cdots x_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$.

Definition 3.4. A polynomial $f(\overline{x})$ is *effectively* 1*-variable* if $f = \tau_1 \cdot g(\tau_2)$, where τ_1, τ_2 are monomials (possibly with negative exponents) and g is a polynomial over U with constant term different from zero.

We denote the x_i-degree of $f(x_1, \ldots, x_n)$ by d_i. Let $\overline{\mu} = (\mu_1, \ldots, \mu_n) \in \mathbb{N}_+^n$. Ritt and Gourin saw the relevance of understanding the ways in which an irreducible polynomial $f(x_1, \ldots, x_n)$ can become reducible once we replace the variables with their powers. Van der Poorten [18] provides a uniform bound for the number of factors of $f(x_1^{\mu_1}, \ldots, x_n^{\mu_n})$ depending only on $D = \max\{d_1, \ldots, d_n\}$. He works over an algebraically closed field of characteristic 0. From an inspection of his proof, one sees that the only property of an algebraically closed field that he uses is that all the roots of

unity belong to the field of coefficients. For the application that we will give of the factorization of an exponential polynomial the coefficients belong to a unique factorization domain containing all roots of unity.

DEFINITION 3.5. A polynomial $f(\overline{x})$ is *power-irreducible* (over K or U) if for each sequence of positive integers $\overline{\mu}$, $f(\overline{x}^{\overline{\mu}})$ is irreducible (over K or U).

Now the fundamental result of Ritt (that if f factors as $f_1 f_2$ then $\mathrm{supp}(f_i) \subseteq \mathrm{supp}(f)$ for $i = 1, 2$) comes into play. A factorization of the exponential polynomial f is equivalent to a factorization of its associate polynomial (over U) into polynomials in fractional powers. Such a factorization of the polynomial is possible iff the polynomial is a unit times a power-reducible polynomial. Looking more closely, one gets an exact correspondence (up to units and associates) between factorization of exponential polynomials and factorizations of compositions of polynomials and powers of variables.

We are now in a position to state a version of a unique factorization result for exponential polynomials, the "Almost Unique Factorization Theorem". As already remarked, the proof in our context follows the lines of the proof of Theorem 2 on page 1296 of [19], and there seems no need to repeat the details.

THEOREM 3.6. *An element $f \neq 0$ of $K[\overline{X}]^E$ factors, uniquely up to units and associates, as a finite product of irreducibles of $K[\overline{X}]$, a finite product of irreducibles of $K[\overline{X}]^E$ whose support is of dimension bigger than* 1*, and a finite product of elements G_j of $K[\overline{X}]^E$, where $\mathrm{supp}(G_{j_1}) \neq \mathrm{supp}(G_{j_2})$ for $j_1 \neq j_2$ and whose supports are of dimension* 1*.*

A very important consequence is that an irreducible f with support of dimension more than 1 is prime. For if f divides gh then by the uniqueness theorem, f must occur in the factorization of one of g or h.

We leave open the interesting question of when f with support of dimension 1 is irreducible.

4. Main result. Zilber's axioms focus on the existence of solutions of certain systems of exponential polynomials. Laczkovich [9] proved that there is no algorithm for testing solvability of systems of exponential polynomials, but the situation is different for a single polynomial. In this section we give a necessary and sufficient condition for an exponential polynomial over a Zilber field to have no zeros in the field. We will show that if the polynomial has a certain form then necessarily it has a zero. This is a special case of some of Zilber's axioms.

For the complex exponential field such a characterization exists and it is due to Henson and Rubel [5]:

Let $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$. Then

$$F(z_1, \ldots, z_n) \text{ has no roots in } \mathbb{C} \quad \text{iff} \quad F(z_1, \ldots, z_n) = e^{G(z_1, \ldots, z_n)},$$

where $G(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

4.1. Constructing strong extensions. First of all we give a method for constructing strong extensions of partial E-domains. In [24] Zilber has a similar result but our proof uses different techniques.

In the following, (R, D, E) will denote a characteristic 0 domain R, $\mathbb{Q} \subseteq R$, with a partial exponential function E defined on R whose domain is D and $\mathbb{Q} \subseteq D$.

LEMMA 4.1. *Let (R, D, E) be a partial E-domain where D is a $\mathbb{Q}$-vector space. Then for any $t \in R$ with $t \notin D$, the partial E-ring R can be extended to a partial E-ring $(S, D \oplus \mathbb{Q} \cdot t, E_1)$, which is also a strong extension. Moreover, $(S, D \oplus \mathbb{Q} \cdot t, E_1)$ can be chosen so that if (R, D, E) satisfies Schanuel's Conjecture then so does $(S, D \oplus \mathbb{Q} \cdot t, E_1)$.*

Proof. We can extend R to S by a transcendental α in such a way that there is a homomorphism from the additive group $(\mathbb{Q}, +)$ into the multiplicative group of S, sending r to α^r. This can be obtained by a simple compactness argument.

Let $D_1 = D \oplus \mathbb{Q} \cdot t$. If $\gamma \in D_1$, then $\gamma = d + rt$, where d and r are uniquely determined with $d \in D$, $r \in \mathbb{Q}$. We extend E to D_1 in the freest possible way as follows:

$$E_1(\gamma) = E(d) \cdot \alpha^r,$$

where $\alpha = E_1(t)$ and each α^r gets its meaning from the homomorphism mentioned above. E_1 extends the morphism E, and satisfies the axioms of exponentiation. Then (S, D_1, E_1) is the extension we wanted.

Now we want to prove that the extension is strong, that is:

(i) $\delta_R(A/B) \leq \delta_S(A/B)$ for any finite subsets A, B of R,
(ii) $\delta_S(B/D_R) \geq 0$ for any $B \subset_{\text{fin}} D_S$.

(i) Simply from the definition of the predimension, we see that to prove (i) we have to show that

$$\text{t.d.}(A \cup B, E_1(A \cup B)) - \text{t.d.}(B, E_1(B)) \geq \text{t.d.}(A \cup B, E(A \cup B)) - \text{t.d.}(B, E(B)).$$

Now, bearing in mind that the domain of exponentiation in S has dimension one more than the dimension of the domain of exponentiation in R, and that $E_1(t)$ is transcendental over R, we see that $E_1(A \cup B)$ has transcendence

degree at most 1 over $E(A \cup B)$, with a similar result for B rather than $A \cup B$.

Now, if t.d.$(B, E_1(B)) =$ t.d.$(B, E(B))$ the estimate above is clear.

If, however, the left-hand side is bigger than the right-hand side, their difference is exactly 1, and then the same is true for t.d.$(A \cup B, E_1(A \cup B))$ and t.d.$(A \cup B, E(A \cup B))$ by the preceding remarks. Thus the inequality holds.

(ii) A similar argument works. Let $A \subseteq D$. We extend A by adding to it the projection of B onto D. Without loss of generality for what follows we can assume this is A, and that B is t. We have to show that $\delta_S(B/A) \geq 0$. But this is obvious since R satisfies (SC) and α is transcendental over R.

Note that the same proof shows that S satisfies (SC). ∎

We can generalize this result to the case of group rings. Using a similar proof the following result holds.

PROPOSITION 4.2. *Let (R, A, E) be a partial E-domain satisfying Schanuel's Conjecture, and let B be an abelian divisible group. If $R_1 = R[t^B]$ and E_1 is the natural extension of E then $(R_1, A \oplus B, E_1)$ is a strong extension of (R, A, E) and satisfies Schanuel's Conjecture.*

4.2. A sharper version of Schanuel's Conjecture for $K[\overline{X}]^E$. We now prove a sharper version of Schanuel's Conjecture for the E-polynomial ring $K[\overline{X}]^E$ where K is a Zilber field. The result is an analogue of what was proved by Ax [1] for power series, and Bianconi [2] for infinitesimal elements of an ultrapower of $\mathbb{C}$.

DEFINITION 4.3. Let $\beta_1, \ldots, \beta_k, \delta_1, \ldots, \delta_n \in K[\overline{X}]^E$, and suppose $\beta_1, \ldots, \beta_k \in R_h$ and $\delta_1, \ldots, \delta_n \in R_j$ with $h < j$. We say that $\delta_1, \ldots, \delta_n$ are $\mathbb{Q}$-*linearly independent over* $\beta_1, \ldots, \beta_k$ if there is no linear combination of $\delta_1, \ldots, \delta_n$ with rational coefficients which belongs to $\langle \beta_1, \ldots, \beta_k \rangle_{\mathbb{Q}}$, the $\mathbb{Q}$-vector space generated by $\beta_1, \ldots, \beta_k$.

We observe that being $\mathbb{Q}$-linearly independent over R_k for some k implies $\mathbb{Q}$-linear independence.

Notice that if $\delta_j = \sum_{i \neq j} r_i \delta_i + \alpha$ with $r_i \in \mathbb{Q}$ and $\alpha \in \langle \beta_1, \ldots, \beta_k \rangle_{\mathbb{Q}}$ then $E(\delta_j)$ is algebraic over $E(\delta_i)$ with $i \neq j$ and $E(\beta_1), \ldots, E(\beta_k)$.

THEOREM 4.4. *Let K be a Zilber field. Suppose that $\gamma_1, \ldots, \gamma_n \in K[\overline{X}]^E - K$ are $\mathbb{Q}$-linearly independent over K. Then*

$$\text{t.d.}_K\, K(\gamma_1, \ldots, \gamma_n, E(\gamma_1), \ldots, E(\gamma_n)) \geq n + 1.$$

Proof. We partition $\gamma_1, \ldots, \gamma_n$ according to the number of iterated exponentials they contain identifying the first partial E-ring they belong to as follows:

$$\gamma_1, \ldots, \gamma_{d_1} \in R_{l_1}; \quad \gamma_{d_1+1}, \ldots, \gamma_{d_2} \in R_{l_2}; \quad \ldots; \quad \gamma_{d_{s-1}+1}, \ldots, \gamma_{d_s} \in R_{l_s}$$

with $d_1 + \cdots + d_s = n$ and $R_{l_1} \subset \cdots \subset R_{l_s}$, where $l_1 \geq 0$.

Without loss of generality we may assume that for each $j = 1, \dots, s-1$, $\gamma_{d_j+1}, \dots, \gamma_{d_{j+1}}$ are $\mathbb{Q}$-linearly independent over the previous γ's, i.e., over $\gamma_1, \dots, \gamma_{d_j}$, and $\gamma_1, \dots, \gamma_{d_1}$ are $\mathbb{Q}$-linearly independent over K.

If not, let $\{\gamma_{h_1}, \dots, \gamma_{h_r}\}$ be a maximal subset of $\{\gamma_{d_j+1}, \dots, \gamma_{d_{j+1}}\}$ which is $\mathbb{Q}$-linearly independent over $\gamma_1, \dots, \gamma_{d_j}$, for $j = 1, \dots, s-1$. If $\gamma \in \{\gamma_{d_j+1}, \dots, \gamma_{d_{j+1}}\} - \{\gamma_{h_1}, \dots, \gamma_{h_r}\}$ then $\gamma \in K(\gamma_1, \dots, \gamma_{d_j}, \gamma_{h_1}, \dots, \gamma_{h_r})$, and $E(\gamma)$ does not contribute towards the transcendence degree of

$$K(\gamma_1, \dots, \gamma_{d_j}, \gamma_{h_1}, \dots, \gamma_{h_r}, E(\gamma_1), \dots, E(\gamma_{d_j}), E(\gamma_{h_1}), \dots, E(\gamma_{h_r}), E(\gamma))$$

over K since it is algebraic over this extension.

Similarly, we can prove that there is no loss of generality in assuming $\gamma_1, \dots, \gamma_{d_1}$ $\mathbb{Q}$-linearly independent over K.

We now show that

$$E(\gamma_1), \dots, E(\gamma_{d_1}); E(\gamma_{d_1+1}), \dots, E(\gamma_{d_2}); \dots; E(\gamma_{d_{s-1}+1}), \dots, E(\gamma_{d_s})$$

are algebraically independent over K. Suppose

$$\sum_I \alpha_I (E(\gamma_1) \cdots E(\gamma_{d_s}))^I = 0 \tag{3}$$

where $I = (n_1, \dots, n_s) \in \mathbb{N}^s$ and $\alpha_I \in K$. We say that a multi-index I is *high* if $n_{d_{s-1}+1}, \dots, n_{d_s}$ are not all equal to 0. If in (3) there is a unique high I then we get a contradiction since we have exponentials of elements of B_{l_s} algebraic over R_{l_s} which contradicts the construction of R_i's (B_{l_s+1} is the R_{l_s}-submodule freely generated by $E(b)$ with $b \in B_{l_s}$). If there are more than one high multi-indices we have to pay attention to possible cancellations. If there is no cancellation then we get a contradiction as before. If there is cancellation then we reduce to work in a lower R_{l_j} where $j < s$, and we get again a contradiction for the same reasons as before. This is also the case when there is no high I.

The extra transcendence degree is given by any of $\gamma_1, \dots, \gamma_{d_1}$ since they do not belong to K. ∎

Remark 4.5. The result of the previous theorem is a special case of Ax's theorem for power series. In our proof we make essential use of the explicit construction of $K[\overline{X}]^E$ as a union of partial E-rings, and we avoid referring to any derivation with constant field K.

4.3. Exponential polynomials with no zeros. Now we state and prove our main result:

Theorem 4.6. *Let $f(\overline{X}) \in K[\overline{X}]^E$ where K is a Zilber field. Then*

$$f(\overline{X}) \text{ has no roots in } K \quad \text{iff} \quad f(\overline{X}) = e^{h(\overline{X})},$$

where $h(\overline{X}) \in K[\overline{X}]^E$.

Proof. One direction is obvious since exponentials have no roots.

Now suppose that f is not an exponential. We show that f has a root in K. Recall that the *height* of f is the first k such that f is in $R_k - R_{k-1}$. If $f \in U = K[\overline{X}]$ then f has a zero in K, unless f is a nonzero constant, in which case f is an exponential. Assume that the height of f is $k+1$ for $k \geq 0$. By the Almost Unique Factorization Theorem, we can reduce the proof to one of the following cases:

Case 1. f is irreducible in $K[\overline{X}]^E$ and $\mathrm{supp}(f)$ has dimension > 1;

Case 2. $\mathrm{supp}(f)$ has dimension 1, i.e. the associated polynomial of f is essentially 1-variable.

In both cases we can assume $f(\overline{X}) \neq e^{h(\overline{X})}g(\overline{X})$ for all $h(\overline{X}), g(\overline{X}) \in K[\overline{X}]^E$, with $\mathrm{height}(g) < \mathrm{height}(f)$ (in particular, $f(\overline{X})$ is not invertible). We will construct a strong extension $\mathcal{A}$ (simply as a partial E-domain) of K in which f has a zero, and there are no new periods. Lemma 2.6 guarantees the existence of an exponential field F which is a strong extension of $\mathcal{A}$, and with no new periods added. By Lemma 2.5, F is also a strong extension of K, and it contains a solution of f. A Zilber field is exponentially-algebraically closed, and so f must have a zero also in K, and this gives the contradiction.

Case 1. Suppose f is irreducible, of height $k+1$, and $\mathrm{supp}(f)$ has dimension more than 1. Let S be the domain $K[\overline{X}]^E/(f)$ (f is prime).

By Theorem 3.6, f divides no element of R_k, and so R_k embeds naturally in S. Now we consider R_k as a partial E-domain, with R_{k-1} as domain of exponentiation. We now put a partial E-domain structure on S, extending that of R_k. We take the representation of f as a series over U, namely

$$f(\overline{X}) = \sum_{i=1}^{n} a_i t^{b_i},$$

where $a_i \in U = R_0$ and $b_i \in B_1 \oplus B_2 \oplus \cdots$. Now some of the b_i are in $R_k - R_{k-1}$. Let D be the $\mathbb{Q}$-space over R_{k-1} generated by all the b_i's. We define E_S on D by $E_S(g) = E(g) + (f)$, i.e. E_S is the natural quotient of the original exponentiation. This is clearly a partial exponentiation, extending that on R_k. We claim that there are no new periods. For, if $E_S(g) - 1$ is divisible by f then for some $c \in K$ and $\mu \in \Gamma$, f divides $ct^\mu - 1$, contradicting the fact that $\mathrm{supp}(f)$ has dimension at least 2 (see Section 3.1).

It is obvious that f has a zero in S. Now we come to the key claim that S is a strong extension of K. For the first condition, since E is total on K we have nothing to prove.

Let B be a subset of $D - K$, assumed, without loss of generality, to be $\mathbb{Q}$-linearly independent over K. Let A be a finite subset of K, linearly

independent over $\mathbb{Q}$. We have to show that

$$\delta_S(B \cup A) - \delta_S(A) \geq 0. \tag{4}$$

By Theorem 4.4 the transcendence degree of $B \cup E_S(B)$ in $K[\overline{X}]^E$ over K is at least one plus the linear dimension of B. If the transcendence degree of $B \cup E_S(B)$ over K drops in S by at most 1 then we are done since we would have

$$\text{t.d.}_{\mathbb{Q}}(B \cup A \cup E(B \cup A)) \geq \text{l.d.}(B) + \text{l.d.}(A),$$

which implies (4). So it is enough to prove that no further algebraic relation for $B \cup E_S(B)$ over K holds in S, except that induced by $f = 0$. Suppose $B = \{\beta_1, \ldots, \beta_t\}$, and $\beta_j = \beta_j^* + \beta_j^{**}$, where $\beta_j^* \in R_{k-1}$ and $\beta_j^{**} \in \langle b_1, \ldots, b_n \rangle_{\mathbb{Q}}$ for $j = 1, \ldots, t$. Without loss of generality for each j we may assume β_j^{**} to be a $\mathbb{Z}$-linear combination of $b_1, \ldots, b_n$ (this hypothesis has no consequences on the transcendence degree). Suppose there is an irreducible polynomial $P(\overline{X}, \overline{Y}) \in K[\overline{X}, \overline{Y}]$ such that

$$P(\beta_1, \ldots, \beta_t, E_S(\beta_1), \ldots, E_S(\beta_t)) = 0. \tag{5}$$

We split each β_j into the two components β_j^* and β_j^{**}. Then by multiplying by a suitable monomial in $E(\beta_1^{**}), \ldots, E(\beta_t^{**})$, we get an algebraic relation satisfied by $E(\beta_1^{**}), \ldots, E(\beta_t^{**})$ over R_k,

$$Q(\beta_1, \ldots, \beta_t, E_S(\beta_1^*), \ldots, E_S(\beta_t^*))(E_S(\beta_1^{**}), \ldots, E_S(\beta_t^{**})) = 0. \tag{6}$$

We may regard $Q(\beta_1, \ldots, \beta_t, E_S(\beta_1^*), \ldots, E_S(\beta_t^*))(\overline{X})$ as a polynomial over R_k^{ff}, the fraction field of R_k. Let $F = R_k^{\text{ff}}$. In this way the polynomial

$$Q = Q(\beta_1, \ldots, \beta_t, E_S(\beta_1^*), \ldots, E_S(\beta_t^*))(E_S(\beta_1^{**}), \ldots, E_S(\beta_t^{**})) \tag{7}$$

is an element of the group ring $F[G]$, where G is the multiplicative group generated by $E_S(\beta_1^{**}), \ldots, E_S(\beta_t^{**})$, and also f is in $F[G]$. So we are in the group ring set-up and we can apply the Almost Unique Factorization of Section 3.1.

From (6) in S it follows that f divides Q of (7) both in $K[\overline{X}]^E$ and in $F[G]$. We factor the polynomial Q in $F[G]$ according to Theorem 3.6, and we find that f divides one of the irreducible factors of Q in $F[G]$. So f is one of these factors, and this implies that f divides Q in $K[\overline{X}]^E$, modulo a monomial. Because of the irreducibility of Q it follows that $Q = f\tau$ for some monomial τ. Hence the transcendence degree of $B \cup E_S(B)$ drops in S at most by 1.

Case 2. (The associate polynomial of) f is essentially 1-variable. Then clearly we can assume without loss of generality that f is of the form

$$H(\overline{X}, t^\tau),$$

where $H(\overline{X}, y)$ is an irreducible polynomial over K, and $\tau \in R_k - R_{k-1}$. We show that, except for the obvious case when H is a constant times a power of the last variable, f has a zero in K.

Let U^{alg} be the algebraic closure of $U = K[\overline{X}]$, and factor H over U^{alg} as

$$\prod_{j=1}^{n} (A_j(\overline{X}) - y) \cdot C(\overline{X}),$$

where the $A_j(\overline{X})$ and $C(\overline{X})$ are in $U^{\mathrm{alg}}[\overline{X}]$, and $C(\overline{X}) \neq 0$. Note that no A_j is zero unless $H = Cy$, when the result is clear. So we assume all $A_j \neq 0$. Now the strategy is to get $E(\tau) = A_j$ for some j, since in this way H has a zero.

Recall that $K[\overline{X}]^E = U[t^G]$ where $G = B_0 \oplus B_1 \oplus \cdots$. This implies $U^{\mathrm{alg}}[t^G] = U[t^G] \otimes_U U^{\mathrm{alg}}$. We consider the extension $S = U[t^G] \otimes_U U^{\mathrm{alg}}$ of K, with domain of exponentiation $D_S = R_{k-1} \oplus \mathbb{Q}\tau$, and we define

$$E_S(\tau) = A_1 \quad (\text{or } A_2, \ldots).$$

We have to give a meaning to $(A_1)^r$ for $r \in \mathbb{Q}$, so that

$$E_S(r.\tau) = (A_1)^r \in U^{\mathrm{alg}}.$$

This is routine, by an inverse limit argument. Then the values of E_S will be in $U^{\mathrm{alg}}[t^G]$. Clearly H has a root is S, and it is left to show that (S, E_S) is a strong extension of K.

We claim there are no new periods. If there are, then for some $r \neq 0$ with $r \in \mathbb{Q}$, $E_S(\alpha + r\tau) = 1$ for some $\alpha \in R_{k-1}$.

This makes A_1 a unit of R_{k+1}, and so of the form ut^δ for some $\delta \in R_k$ and $u \in U$. Since t^δ is transcendental over U unless $\delta = 0$, we conclude that A_1 is a unit of U, and so in K. Then, up to a nonzero constant of K, H is $A_1 - y$ (if there are new periods). So the equation $f = 0$ is essentially $t^\tau = A_1$. This is equivalent to solving $\tau = a + p$, where $a \in K$ and $E(p) = 1$. Since τ is in R_k we can apply the inductive hypothesis of Case 1, and we can deduce, for any period p, $\tau = a + p$ is solvable in K unless $\tau - a - p$ is of the form e^q for some $q \in K[\overline{X}]^E$. Maybe this can happen for some p, but it cannot happen for distinct periods p_1 and p_2. For then we would get an equation $t^{q_1} - t^{q_2} = p_1 - p_2$, and from the normal form of exponential polynomials it follows that no such equation is solvable in $K[\overline{X}]^E$. So we can solve $\tau = a + p$ in K for some period p, and thus we solve $t^\tau = A_1$ in K as required.

This leaves us the case when no new periods are introduced. We want to show that S is a strong extension of K. The first condition for strong holds, since exponentiation is total on K. For the second condition, we argue as in Case 1.

Let A be a finite subset of K, linearly independent over $\mathbb{Q}$, and of dimension q. Let B be a finite subset of $D_S - K$, and assume, without loss of generality, that B is $\mathbb{Q}$-linearly independent over K. A typical element of B is of the form $\mu_i = \nu_i + \tau_i$, with $\nu_i \in R_{k-1}$ and $\tau_i \in \mathbb{Q}\tau$. If distinct μ_i's have nonzero τ_i's, then we can make a change of variable to make one of the τ_i zero. So, without loss of generality, at most one τ_i is nonzero. If all τ_i are zero, we can just use the fact that R_k is a strong extension of K, and complete the proof. If precisely one is nonzero, let C_0 be the subset of B consisting of the μ_i's with corresponding $\tau_i = 0$. Then C_0 is $\mathbb{Q}$-linearly independent over K, and so by Theorem 4.4 the transcendence degree of $C_0 \cup E_S(C_0)$ over K is at least the $\mathbb{Q}$-dimension of B over K, provided C_0 is nonempty. This proves that the predimension in S of $A \cup B$ does not go below q, unless B_0 is empty. Finally, we consider the case when C_0 is empty, i.e. when B is a singleton with element (without loss of generality) $\nu + \tau$. Since this element is transcendental over K it is clear that the predimension does not go below q. This completes the proof. ∎

Remark 4.7. In the proof of Theorem 4.6 we used only purely algebraic methods. The few cases where some of Zilber's axioms have been proved for the complex exponential field use hard complex analysis, e.g. Nevanlinna theory.

4.4. Picard's Little Theorem. A consequence of the characterization proved in Theorem 4.6 is a classical result for the complex exponential field, namely, Picard's Little Theorem for exponential polynomials over a Zilber field.

First of all we observe that as a corollary of Theorem 4.6 the map which associates to every polynomial in $K[\overline{X}]^E$ the corresponding function $K^n \to K$ is 1-1. Let $f, g \in K[\overline{X}]^E$ be such that $f(\overline{a}) = g(\overline{a})$ for all $\overline{a} \in K^n$. If $c_1, c_2 \in K$ are nonzero elements of K and $c_1 \neq c_2$ then by Theorem 4.6,

$$f(\overline{X}) - g(\overline{X}) - c_1 = e^{h_1(\overline{X})} \quad \text{and} \quad f(\overline{X}) - g(\overline{X}) - c_2 = e^{h_2(\overline{X})}$$

for some $h_1, h_2 \in K[\overline{X}]^E$. This implies

$$c_2 - c_1 = e^{h_1(\overline{X})} - e^{h_2(\overline{X})},$$

which is clearly a contradiction. Note that in the case of $\mathbb{C}$ a derivation is used (see [3]).

Theorem 4.8. *A nonconstant polynomial $f(x) \in K[x]^E$ cannot omit two values.*

Proof. Let $f(x) \in K[x]^E$, and suppose by contradiction that for some $a, b \in K$, $a \neq b$, $f(x) \neq a, b$ for all $x \in K$. Then the corresponding function

$$g(x) = \frac{f(x) - a}{b - a}$$

is different from 0 and 1 for all $x \in K$. From $g(x) \neq 0$ for all $x \in K$ and Theorem 4.6 it follows that

$$g(x) = e^{h(x)},$$

where $h(x)$ is nonconstant polynomial in $K[x]^E$. Moreover, $g(x) \neq 1$, for all $x \in K$, and this implies that $g(x) - 1 = e^{l(x)}$ for some nonconstant $l(x) \in K[x]^E$; hence we get $e^{h(x)} - e^{l(x)} = 1$, which is a contradiction. ∎

4.5. Polynomials with finitely many zeros. Another consequence of our main result is the following characterization of those exponential polynomials which have only finitely many zeros.

THEOREM 4.9. *A nonconstant polynomial $f(x) \in K[x]^E$ has always infinitely many zeros unless it is of the form*

$$f(x) = (x - \alpha_1)^{n_1} \cdots (x - \alpha_s)^{n_s} e^{g(x)} \tag{8}$$

where $\alpha_1, \ldots \alpha_s \in K$, $n_1, \ldots, n_s \in \mathbb{N}$ and $g(x) \in K[x]^E$.

Proof. Since the product of two polynomials as in (8) is still of the same form, it is enough to prove the statement for irreducible polynomials with support of dimension greater than 1, and for polynomials with 1-dimensional support, according to the Almost Unique Factorization Theorem. Let $\alpha_1, \ldots, \alpha_k$ be the roots of f in K. We go through the proof of Theorem 4.6 and we use the same notation.

Suppose f is irreducible and $\dim(\mathrm{supp}(f)) > 1$. We constructed a strong extension S of K in which f has a root which is necessarily different from α_i for $i = 1, \ldots, k$. This property can be expressed by an existential statement, and so it is also true in K, which gives a contradiction.

If $\dim(\mathrm{supp}(f)) = 1$ then f may be considered as a polynomial $H(x, t^\tau)$, where $H(x, y)$ is an irreducible polynomial over K. Now H is factorized over U^{alg} ($U = K[x]$) as

$$\prod_{j=1}^{n} (A_j(x) - y) \cdot C(x),$$

where the $A_j(x)$ and $C(x)$ are in U^{alg}, and $C(x) \neq 0$. In the strong extension we considered we had the choice of defining $E(\tau) = A_j$ for some j. If for some j_0 no new periods are added then we define $E(\tau) = A_{j_0}$, and we have a new root of f in S. We can then argue as before. If for all j new periods are added then $H(x, y)$ is reducible over K. This forces $H(x, y) = A(x) - y$ since H is irreducible over K. Then we get infinitely many zeros of f in K by solving $\tau = a + p$ for some $a \in K$ and p a period of K. ∎

REMARK 4.10. This result is not known for the complex exponential field.

Acknowledgments. We are grateful to the anonymous referee both for initial comments and for a speedy response to the revised version.

References

[1] J. Ax, *On Schanuel's conjecture*, Ann. of Math. 93 (1971), 252–268.
[2] R. Bianconi, *Some remarks on Shanuel's conjecture*, Ann. Pure Appl. Logic 108 (2001), 15–18.
[3] L. van den Dries, *Exponential rings, exponential polynomials and exponential functions*, Pacific J. Math. 113 (1984), 51–66.
[4] E. Gourin, *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*, Trans. Amer. Math. Soc. 32 (1930), 485–501.
[5] C. W. Henson and L. A. Rubel, *Some applications of Nevanlinna Theory to Mathematical Logic: identities of exponential functions*, Trans. Amer. Math. Soc. 282 (1984), 1–32.
[6] E. Hrushovski, *A new strongly minimal set*, Ann. Pure Appl. Logic 62 (1993), 147–166.
[7] —, *Strongly minimal expansions of algebraically closed fields*, Israel J. Math. 79 (1992), 129–151.
[8] J. Kirby, *Exponential algebraicity in exponential fields*, arXiv:0810.4285v2 [math.LO], 2008.
[9] M. Laczkovich, *The removal of π from some undecidable problems involving elementary functions*, Proc. Amer. Math. Soc. 131 (2002), 2235–2240.
[10] S. Lang, *Algebra*, Springer, 2002.
[11] L. A. MacColl, *A factorization theory for polynomials in x and in functions $e^{\alpha x}$*, Bull. Amer. Math. Soc. 41 (1935), 104–109.
[12] A. Macintyre, *Exponential algebra*, in: Logic and Algebra, to the memory of Roberto Magari (A. Ursini et al., eds), Lecture Notes in Pure Appl. Math. 180, Dekker, 1991, 191–210.
[13] —, *Lecture Notes on Exponentiation*, Urbana, 1985, unpublished.
[14] A. Macintyre and A. Wilkie, *On the decidability of the real exponential field*, in: Kreiseliana: about and around Georg Kreisel, A. K. Peters, 1996, 441–467.
[15] D. Marker, *A remark on Zilber's pseudoexponentiation*, J. Symbolic Logic 71 (2006), 791–798.
[16] —, *Model Theory: An Introduction*, Springer, 2002.
[17] Yu. V. Nesterenko, *Modular functions and transcendence questions*, Sbornik Math. 187 (1996), 1319–1348.
[18] A. J. van der Poorten, *Factorisation in fractional powers*, Acta Arith. 70 (1995), 287–293.
[19] A. J. van der Poorten and G. R. Everest, *Factorisation in the ring of exponential polynomials*, Proc. Amer. Math. Soc. 125 (1997), 1293–1298.
[20] J. F. Ritt, *A factorization theorem of functions $\sum_{i=1}^{n} a_i e^{\alpha_i z}$*, Trans. Amer. Math. Soc. 29 (1927), 584–596.
[21] G. Terzo, *Some consequences of Schanuel's conjecture in exponential rings*, Comm. Algebra 36 (2008), 1171–1189.
[22] B. Zilber, *The structure of models of uncountably categorical theories*, in: Proc. Int. Congress of Math., Warszawa, Vol. 1, 1984, 359–368.

[23] B. Zilber, *Analytic and pseudo-analytic structures*, in: Logic Colloquium 2000, Lecture Notes in Logic 19, Assoc. Symbolic, Urbana, IL, 2005, 392–408.

[24] —, *Pseudo-exponentiation on algebraically closed fields of characteristic zero*, Ann. Pure Appl. Logic 132 (2004), 67–95.

Paola D'Aquino, Giuseppina Terzo
Department of Mathematics
Seconda Università di Napoli
Via Vivaldi 43
81100 Caserta, Italy
E-mail: paola.daquino@unina2.it
giuseppina.terzo@unina2.it

Angus Macintyre
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS, UK
E-mail: angus@dcs.qmul.ac.uk

Received 24 November 2008;
in revised form 6 November 2009