Annals of Pure and Applied Logic 167 (2016) 901–938

Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

www.elsevier.com/locate/apal

Turing meets Schanuel ☆

Angus Macintyre

QMUL, United Kingdom

ARTICLE INFO

Article history:
Received 7 January 2015
Received in revised form 20 June 2015
Accepted 10 July 2015
Available online 16 June 2016

MSC:
03C60
11U09
03D45

Keywords:
Schanuel Conjecture
Exponential fields
Computable models

ABSTRACT

I show that all Zilber's countable strong exponential fields are computable exponential fields.

1. Introduction

Turing [52] applied Tarski's decidability of the theory of real closed fields to the decision problem for solvability of equations in Lie groups. I do not know if he knew Tarski's problem on the decidability of the real exponential, but his strengths in analysis [50] would certainly have equipped him to confront this problem, and indeed Zilber's more recent problems [60] on the complex exponential. It seems to me likely that he would have appreciated the work of the last 25 years on the logic of the real and complex exponentials [59,37,60]. In this paper I consider Schanuel's Conjecture, now fundamental to our understanding of the logic of the real and complex exponentials, from the standpoint of Turing computability. This reveals many challenging problems, some of which I solve. These will be revealed below. The following is one example.

Theorem. *Schanuel's Conjecture for the complex exponential is equivalent to the version in which one quantifies only over computable complex numbers, i.e. numbers of the form $a + ib$ where a, b are computable reals.*

☆ This work was partially supported by a generous Leverhulme Emeritus Fellowship.
E-mail address: a.macintyre@qmul.ac.uk.

http://dx.doi.org/10.1016/j.apal.2015.10.003

This is related to the beautiful result of Kirby and Zilber [31] on the uniform Schanuel Conjecture for the real exponential field. Another main result of the present paper, given in the last section as Theorem 8.3, is:

Theorem. *Each of the countable strongly existentially closed exponential fields of Zilber is a computable exponential field.*

The proof of this is quite demanding, because of the paucity of modern foundational material on computable algebra and algebraic geometry. It is notable that no analogue of this theorem is known for models of the theory of the complex exponential field.

2. Preliminaries about the basic real structures

The "structures mères" are the real exponential field $\mathbb{R}_{\exp}$ and the complex exponential field $\mathbb{C}_{\exp}$. These are naturally construed as structures for the language of exponential rings, with the usual primitives $+, -, \cdot, 0, 1, E$. The basic equational axioms [54] are

(1) axioms for commutative unital rings;
(2) $E(0) = 1$;
(3) $E(x + y) = E(x)E(y)$

There is by now a sizable literature on these E-rings. For earlier work one should consult [54,36]. For a more recent treatment, one should consult the very useful papers [28,29] by Jonathan Kirby.

2.1. Decidability

The decidability of $\mathbb{R}_{\exp}$ has been a very influential problem in mathematical logic. Over the years, the structure of definable relations in $\mathbb{R}_{\exp}$ became the focal problem, and this led to the large-scale study of o-minimal theories [55], one of the outstanding successes of model theory.

What we currently know about $Th(\mathbb{R}_{\exp})$ is that it is unconditionally model-complete [59] and o-minimal, and both constructively model complete (i.e. there is an algorithm which given a formula produces an existential formula equivalent to it over the theory) and decidable if Schanuel's Conjecture for $\mathbb{R}$ is true [37]. We also know a relative of Schanuel's Conjecture [37] equivalent to the decidability of $Th(\mathbb{R}_{\exp})$. I do not expect to see an unconditional proof of the decidability of $Th(\mathbb{R}_{\exp})$. There are, however, unconditional upper bounds on the Turing degree of $Th(\mathbb{R}_{\exp})$ (see Corollary 2.1 below).

2.2. Restricted analytic functions

Understanding $Th(\mathbb{R}_{\exp})$ has been greatly facilitated by the study of related systems connected to subanalytic sets [55,22]. The simplest of these systems is the real field, with the following restricted exponential $E \restriction [0, 1]$ satisfying:

$E \restriction [0, 1](x) = exp(x)$ if $|x| \leq 1$
$E \restriction [0, 1](x) = 0$ if $|x| > 1$.

Let $\mathbb{R}_{\exp\restriction[0,1]}$ be the real field with this structure, in the language for ordered exponential rings. It is obvious that $\mathbb{R}_{\exp\restriction[0,1]}$ is definable in $\mathbb{R}_{\exp}$, and so o-minimal, and it is known [17] that $\mathbb{R}_{\exp}$ is <u>not</u> interpretable in $\mathbb{R}_{\exp\restriction[0,1]}$.

It will be convenient to consider each of the enrichments $\mathbb{R}_{\exp\restriction[0,n]}$ of $\mathbb{R}$, for $n \in \omega$, got by adjoining $E \restriction [0, n]$, which is exp on $[0, n]$ and 0 elsewhere on the positive real line. It is quite clear that each of these is bi-interpretable with $\mathbb{R}_{\exp\restriction[0,1]}$, and inherits o-minimality from $\mathbb{R}_{\exp}$. We have good reason also to consider the enrichment of $\mathbb{R}$ by all $\mathbb{R}_{\exp\restriction[0,n]}$ at once. Write this as $\mathbb{R}_{\exp\restriction[0,n]}, n \in \omega$. This is obviously bi-interpretable with $\mathbb{R}_{\exp\restriction[0,1]}$, and o-minimal, and by [17] does not interpret $\mathbb{R}_{\exp}$.

2.3. Trigonometric functions

Of greater importance in this paper are the systems involving restricted *sine* and *cosine*. The importance of these is first evident in [17]. We start with sine and cosine on the real line, and restrict each to various compact $[0, n]$, just as we did with exp (putting the function equal to 0 outside the compact set). Using these and the restriction of exp as above, we get the enrichments $\mathbb{R}_{\exp\restriction[0,n],\cos\restriction[0,n],\sin\restriction[0,n]}$, and, putting all these together,

$$\mathbb{R}_{\exp\restriction[0,n],\cos\restriction[0,n],\sin\restriction[0,n]}, \quad n \in \omega.$$

It is easy, using addition formulas, to show that the latter is bi-interpretable with $\mathbb{R}_{\exp\restriction[0,1],cos\restriction[0,1],sin\restriction[0,1]}$. Moreover $\mathbb{R}_{\exp\restriction[0,n],\cos\restriction[0,n],\sin\restriction[0,n]}, n \in \omega$ is o-minimal, say by [17]. However, one has the quite deep result of [9] that $\mathbb{R}_{\exp\restriction[0,1],\cos\restriction[0,1],\sin\restriction[0,1]}$ is <u>not</u> interpretable in $\mathbb{R}_{\exp\restriction[0,1]}$. One naturally adds unrestricted exp to the above restricted theories, giving the obvious $\mathbb{R}_{\exp,\cos\restriction[0,n],\sin\restriction[0,n]}, n \in \omega$. This is o-minimal, a very important result, proved in [57] and in the later [56]. This structure is <u>not</u> interpretable in $\mathbb{R}_{\exp}$ by [9].

One final enrichment that inevitably comes to mind is $\mathbb{R}_{\exp,\cos,\sin}$, in which we take the globally defined exp, cos and sin as primitives. From my perspective, this is a very wild theory. Because of its relevance to a still not excluded nasty scenario about $\mathbb{C}_{\exp}$ (see 5.1) I spell out some of the complications (of which many are folklore).

Theorem 2.1. $\mathbb{R}_{\exp,\cos,\sin}$ *is not o-minimal.*

Proof. $\mathbb{Z}$ is definable in $\mathbb{R}_{\exp,\cos,\sin}$ as

$$\{x : (\forall w)\,(\cos w = 1 \to \cos(xw) = 1)\} \qquad \square$$

Note that in this we use only cos (and not exp) in the above definition, and thereby show that cos is not definable in $\mathbb{R}_{\exp}$. In contrast, I sketch below a proof that exp is definable from cos.

Once one has, as above, an interpretation of the structure $\mathbb{R}_{\mathbb{Z}}$ consisting of the field $\mathbb{R}$ with the subset $\mathbb{Z}$ distinguished, one readily uses individual reals to code arbitrary subsets of $\mathbb{N}$ (e.g. using dyadic expansion of reals). I outline the details. For $r \in \mathbb{R} \cap [0, 1]$ we define $Set_\omega(r)$ as the set of $n \in \mathbb{Z}$ such that $n \geq 0$ and

$$(2^n) - [2^n \cdot r] \geq \frac{1}{2}.$$

Here $[x]$ is the usual integer part of x. Certainly $r \to Set_\omega(r)$ is definable in $\mathbb{R}_{\mathbb{Z}}$ and $Set_\omega(r)$ is a subset of $\mathbb{N}(= \omega)$. If

$$r = \sum_{k=0}^{\infty} a_k 2^{-(k+1)}$$

with $a_n = 0$ or 1 (as is always possible for $r \in [0, 1]$) then

$$2^n r = \sum_{k=0}^{n-1} a_k 2^{n-(k+1)} + a_n 2^{-1} + \sum_{k>n} a_k 2^{n-(k+1)}. \tag{$\sharp$}$$

The first term is an integer $\leq 2^n r$, and the last is $\leq \frac{1}{2}$, with equality only if $a_k = 1$ for $k > n$, $a_n 2^{-1}$ is 0 or $\frac{1}{2}$ according as $a_n = 0$ or 1. Suppose $r \notin \mathbb{Q}$. Then we do not have $a_k = 1$ for all $k > n$. In this case the last term is $< \frac{1}{2}$. So if $a_n = 0$ then $n \notin Set_\omega(r)$. If $a_n = 1$ then $a_n \cdot \frac{1}{2} = \frac{1}{2}$ and thus $n \in Set_\omega(r)$. Thus if $r \notin \mathbb{Q}$,

$$Set_\omega(r) = \{n : a_n = 1\}.$$

What if $r \in \mathbb{Q}$, and all but finitely many a_n are 1? Choose n_0 minimal so that $a_k = 1$ for all $k > n_0$. (If $a_k = 0$ for all k then $r = 0$ and $Set_\omega = \emptyset$.) Then if $n < n_0$ and $a_n \neq 0$ then $n \notin Set_\omega(r)$ by ($\sharp$). If $n < n_0$ and $a_n = 1$ then $n \in Set_\omega(r)$ by ($\sharp$). If $n \geq n_0$ then ($\sharp$) becomes

$$2^n r = \sum_{k=0}^{n-1} a_k 2^{n-(k+1)} + a_n 2^{-1} + \frac{1}{2}.$$

Thus if $a_n = 0$ then $n \notin Set_\omega(r)$. But if $a_n = 1$ then $2^n r - [2^n r] = 0 < \frac{1}{2}$, so also $n \notin Set_\omega(r)$. Thus

$$Set_\omega(r) = \{n : a_n = 1\} \cap \{n : n < n_0\}.$$

So

Lemma 2.1.

$$\{Set_\omega(r) : r \in [0,1]\} = \{X : X \subset \mathbb{N}\}$$

Proof. Done. □

We deduce:

Theorem 2.2. $\mathbb{R}_\mathbb{Z}$ *interprets full second-order arithmetic.*

Proof. Done. □

Second-order arithmetic is carefully explained in [2], as an axiomatic theory in a two-sorted logic, corresponding to an arithmetic structure and a Boolean algebra of subsets. Full second-order arithmetic is the theory of the standard integers and its powerset. Later I shall have more to say on connections between complex exponentiation and second-order arithmetic. One can readily see from the preceding proof that every projective relation [26] on $\mathbb{R}$ is definable (maybe with parameters) in $\mathbb{R}_\mathbb{Z}$, and thus in $\mathbb{R}$ with cos as an extra primitive. It is an instructive exercise to show in this way that exp is (parameter-free) definable from cos in $\mathbb{R}$. It is very easy to see, using Euler that exp is definable from cos in $\mathbb{C}$. We return to this later.

2.4. Model-completeness and decidability for the preceding enrichments

For the subanalytic enrichments introduced earlier (i.e. those with primitives defined only on compact sets), one has the following unconditional result.

Theorem 2.3. *Let T be the theory of any one of the structures*

$$\mathbb{R}_{\exp\restriction[0,n], n\in\omega}, \mathbb{R}_{\cos\restriction[0,n], \sin\restriction[0,n], n\in\omega}, \mathbb{R}_{\exp\restriction[0,n], \cos\restriction[0,n], \sin\restriction[0,n], n\in\omega}.$$

Then T is computably model-complete (in the sense that there is a computable function taking formulas to T-equivalent existential formulas). Moreover, in each case one identifies a computable subset T_0 of T such that the preceding computable function produces a T_0-equivalent formula.

Proof. The proof given for $\mathbb{R}_{\exp\restriction[0,1]}$ in [37] adapts routinely, because the primitives are Pfaffian. However, to avoid confusion, I make some comments about the formalism actually used by Wilkie in [58]. Rather than $\exp \restriction [0,1]$ Wilkie uses the total real analytic primitive

$$e(x) = \exp\Big(\frac{1}{1+x^2}\Big)$$

and it is for this he proves model-completeness and in [58] gets Theorem 2.2. But the choice of primitives does not matter here, as I now explain.

The first and most essential issue is to pass back and forth between $e(x)$ and $\exp \restriction [0,1]$ using definitions which are both existential and universal. I simply list the relevant definitions:

1.

$$\begin{gathered}
\exp \restriction [0,1](x) = y \iff \\
(\exists t)\Big(x = \frac{1}{1+t^2} \wedge e(t) = y\Big) \vee (x = 0 \wedge y = 1) \vee (x < 0 \wedge y = 0) \vee (x > 1 \wedge y = 0) \\
\iff (0 < x \leq 1) \wedge (\forall t)\Big[x = \frac{1}{1+t^2} \to e(t) = y\Big] \\
\vee (x = 0 \wedge y = 1) \vee (x < 0 \wedge y = 0) \vee (x > 1 \wedge y = 0)
\end{gathered}$$

2.

$$\begin{gathered}
e(t) = y \\
\iff \exp \restriction [0,1]\Big(\frac{1}{1+t^2}\Big) = y \\
\iff \exists w(w(1+t^2) = 1 \wedge \exp \restriction [0,1](w) = y) \\
\iff \exists w(w(1+t^2) = 1 \to \exp \restriction [0,1](w) = y)
\end{gathered}$$

An entirely analogous argument works for $\cos \restriction [0,1]$ and $\cos(\frac{1}{1+t^2})$, etc.

Thus (constructive) model-completeness for the two formalisms is equivalent, and the same is true for restricted sin and cos. $\square$

2.5. Deciding the existential theory

In due course I will bring Schanuel's Conjecture to bear on this problem, but first I give an unconditional bound for the Turing complexity of the existential theory. For the structures just considered this will combine with the preceding theorem to give unconditional bounds for the Turing degree of their first-order theories.

Let M be one of the structures in the statement of the last theorem, T its theory, and T_0 the recursive subtheory specified in the theorem. The first step is to note that we have a computable function taking existential sentences ψ to existential sentences equivalent over T_0 to the negation of ψ. Next, since we are in $\mathbb{R}$, and by using standard devices of adding extra variables to eliminate nesting of terms, we can, as far as the decision problem is concerned, restrict to existential ψ of the form

$$(\exists x_1, \ldots, x_n)[P(x_1, \ldots, x_n, \tau_1(x_1), \ldots, \tau_n(x_n)) = 0]$$

where P is a polynomial over $\mathbb{Z}$ in $x_1, \ldots, x_n, y_1, \ldots, y_n$, and each $\tau_j(x)$ is one of the subanalytic primitives (i.e. some $\mathbb{R}_{\exp\restriction[0,m]}$, or $\cos \restriction [0, m]$, or $\sin \restriction [0, m]$). Now, by inspecting each τ_j to see which m occurs, one can (computably) pass to an equivalent ψ of the form

$$(\exists x_1, \ldots, x_n)[P(x_1, \ldots, x_n, \gamma_1(x_1), \ldots, \gamma_n(x_n)) = 0],$$

P a polynomial over $\mathbb{Z}$, and the γ unrestricted exp, cos or sin. (Hint: If $\tau_1 = \exp \restriction [0, m]$, go to

$$(\exists x_1, \ldots, x_n)[0 \le x_1 \le m \wedge P(x_1, \ldots, x_n, \tau_1(x_1), \ldots, \tau_n(x_n)) = 0]$$
$$\vee[\neg(0 \le x_1 \le m) \wedge P(x_1, \ldots, x_n, 0, \ldots, \tau_n(x_n)) = 0]$$

replace disjunction of equations by a single one, and proceed by induction to modify the later τ.)

Now write $P^*(x_1, \ldots, x_n)$ for $P(x_1, \ldots, x_n, \gamma_1(x_1), \ldots, \gamma_n(x_n))$ as above. ψ is true if and only if $P^* = 0$ has a solution in some polydisc

$$D_A = \{(x_1, \ldots, x_n) : |x_j| \le A, \text{ for each } j\},$$

where $A > 0$ is in $\mathbb{N}$.

By a straightforward argument in computable (real or complex) analysis, one gets a computable SW ("Stone–Weierstrass") which on inputs P^* as above and positive rationals A, ε produces a polynomial

$$SW(P^*, A, \varepsilon)$$

over the rationals such the supremum of

$$|P^* - SW(P^*, A, \varepsilon)|$$

is less than ε on D_A.

Then P^* is solvable in D_A if and only if

$$(\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0)\ (\exists (x_1, \ldots, x_n) \in D_A)|SW(P^*, A, \varepsilon)(x_1, \ldots, x_n)| < \varepsilon.$$

Now, bearing in mind Tarski's computable quantifier elimination for $\mathbb{R}$, this is computably equivalent to a Π^0_1 condition in A. Now existentially quantify over A, to conclude:

Theorem 2.4. *The decision problem for existential sentences of* $\mathbb{R}_{\exp,\cos,\sin}$ *is* $\le 0''$.

Proof. Use just one half of the preceding analysis. $\square$

However, for the restricted cases we have unconditional computable model completeness, and the preceding argument gives that the existential theory and its complement are both Π^0_2, so

Theorem 2.5. *For T as in Theorem 2.3, the Turing degree of the existential theory, and thus of the theory, is* $\le 0'$

Proof. Use the preceding theorem, and the preceding discussion. $\square$

Corollary 2.1. $Th(\mathbb{R}_{\exp})$ *has Turing degree* $\le 0'$.

Proof. This is immediate from Ressayre's great theorem [42] that $Th(\mathbb{R}_{\exp})$ is axiomatized by $Th(\mathbb{R}_{\exp} \restriction [0,1])$ and a recursive set of axioms. $\square$

Note. Later we will spell out Laczkovich's argument [33], which shows that the decision problem for existential sentences of $\mathbb{C}_{\exp}$ is $\geq 0'$, which will give an exact bound $0'$ when combined with a complex variable variant of the above, using again restricted model-completeness. We will see also a further subtlety relating to solvability of single equations, an issue not arising in the real case.

3. The role of Schanuel's Conjecture

3.1.

Let S be any exponential domain of characteristic 0. We say S satisfies the Schanuel Condition (SC) iff

Whenever $s_1, \ldots, s_n \in S$, are linearly independent over $\mathbb{Z}$, then the transcendence degree over $\mathbb{Q}$ of $(s_1, ..., s_n, E(s_1), ..., E(s_n))$ is at least n.

An equivalent version, more common since [60] is to drop the condition of linear independence and to replace the last n by the linear dimension over $\mathbb{Q}$ of $(s_1, ..., s_n, E(s_1), ..., E(s_n))$.

When $S = \mathbb{C}$, with the usual E, SC is the famous unproved Schanuel's Conjecture.

In [35] there is an early result connecting Schanuel's Conjecture to exponential algebra and computational problems about exponential constants. [35] was influenced by earlier work of Caviness and Prelle [12] and Shackell [46]. In [37], which starts from Wilkie's great work of 1991 [59], the Schanuel Conjecture for $\mathbb{R}$ is used in a more subtle way.

Theorem 3.1. *(1) If SC holds for $\mathbb{R}$ then $\mathbb{R}_{\exp\restriction[0,n],n\in\omega}$ is decidable. (2) If SC holds for $\mathbb{R}$ then $\mathbb{R}_{\exp}$ is computably model complete and decidable. (3) If SC holds for $\mathbb{C}$ then $\mathbb{R}_{\exp\restriction[0,n],\cos\restriction[0,n],\sin\restriction[0,n],n\in\omega}$ is decidable. (4) If SC holds for $\mathbb{C}$ then $\mathbb{R}_{\exp,\cos\restriction[0,n],\sin\restriction[0,n],n\in\omega}$ is computably model-complete and decidable.*

Proof. (1) and (2) are in [37]. (3) and (4) are unpublished results of Macintyre and Wilkie, and can be proved by rather direct modifications of the methods of [37]. $\square$

3.2. Computable and definable reals

Turing's original paper [51] remains very congenial to me, and what I have to say about computable analysis in this paper fits easily with his foundations. Still, there has been some justified criticism of his pioneering work, and agreeable discussion in both [4] and [23]. One should be aware of such work, and of the diverse efforts of those who have contributed to computable analysis over the last 80 years, but my excuse for being informal is that I am dealing with very classical entire functions such as exp and sin, where one knows such explicit and copious computable information that no general theory is required. Thus I am going to work with an unspecified notion of computable real number, and computable complex number, with a typical goal of showing that some complex numbers arising in my analysis are computable. I doubt that what I do will disturb any philosophy of computable analysis (but if it does, something interesting will be going on).

Theorem 3.2 below is probably known only to a few experts, but it deserves to be better known. It depends on Wilkie's [59,58] all-important characterization of definable functions, applicable to a wide range of o-minimal (specifically Pfaffian) situations. After Zilber's work [60] Wilkie-definability emerged in a broader setting. Firstly, one moved from real to complex situations, and then, in the setting of Zilber's work on the model theory of the Schanuel condition, to exponential fields with no overt analytic structure, but rich exponential structure.

The original structures we study are enrichments of the real or complex fields (and later we work over more general real-closed or algebraically closed fields). The basic extra primitives might include $<$ on $\mathbb{R}$ or $|z|$ on the complexes, but the most important ingredients are various $f(x_1, \dots, x_n)$ corresponding to total analytic functions of various arities. The restricted functions considered earlier may occur too, but may equally be replaced in the real case (as in [58]) by totally defined analytic primitives, without changing the basic results on definability. In the earlier cases we had only unary primitives, but this was accidental.

We consider Hovanski Systems in the primitives. These consist of n equations in n unknowns $x_1, \dots, x_n$, with parameters $w_1, \dots, w_k$. The basic equations are of the form $F_j(x_1, \dots, x_n, w_1, \dots, w_k) = 0$ for $1 \leq j \leq n$, where each F is of the form

$$P(x_1, \dots, x_n, f_1(x_{s_1(1)}, \dots, x_{s_1(l_1)}), \dots, f_n(x_{s_n(1)}, \dots, x_{s_n(l_n)}), w_1, \dots, w_k)$$

where P is a polynomial over the rationals in $(x_1, \dots, x_n, y_1, \dots, y_n, w_1, \dots, w_k)$, the f_j are analytic primitives of respective arities l_j, and the s_j are functions respectively from $1, \dots, l_j$ into $1, \dots, n$.

For the systems we consider, the notion of partial derivative of a primitive can be defined formally (e.g. for exp) as a term of the system, and then it is natural to consider models with no visible analytic structure. In this way the notion of Jacobian (matrix) of a system makes sense, as does the notion of a Hovanski System, which is defined as a system of the above form with the added condition that the Jacobian determinant, with respect to $x_1, \dots, x_n$ is nonzero. Of course such systems are familiar in analytic or algebraic–geometric situations, in the realm of the Implicit Function Theorem or étale covers. Here we call them Hovanski Systems because of the fundamental role of Hovanski's work [27] in opening up the wonderful landscape of o-minimality.

Hovanski proved in [27], for $\mathbb{R}$ a very general result on Pfaffian primitives (which subsumes the case of exp and restricted cos and sin saying that there is a computable d which on input a Hovanski system $\Sigma(x_1, \dots, x_n, w_1, \dots, w_n)$ produces an integer bound for the number of real solutions independent of the choice of parameters $(w_1, \dots, w_n)$. This was crucial for Wilkie's work. For $\mathbb{C}$, with exp, all one can say is that the zeros are isolated in the complex topology, and so form a countable set (which may be infinite, as the set of zeros of exp shows).

We now come to a definition of enormous importance. The history is interesting. The notion is practically explicit in Wilkie [58,59], and this led me to put down, in [35] a generalization to the complex case, without my being able to prove much about it. With the arrival of Zilber on the exponential scene [60], the landscape changed. Independently Kirby, Wilkie and I saw the equivalence of Zilber's closure to one based on Hovanski systems. This, and a lot more, is beautifully explained in Kirby's work [28], which is indispensable for much of the rest of my paper.

The definition is relative to an exponential field, possibly with extra structure. The basic definition makes sense in any situation, not necessarily analytic like $\mathbb{R}$ or $\mathbb{C}$, where the basic apparatus of partial differentiation is available. We will begin by proving theorems for various structures on $\mathbb{R}$ (and related o-minimal structures), and later consider it for the complex field and the Zilber fields [60]. When we need to assume that we are in a Pfaffian o-minimal setting, we add (Pfaff) as a hypothesis in Theorem 3.2. For now, in real settings, we apply the methods below to the real structures discussed above, except for the "wild" $\mathbb{R}_{\exp,\cos,\sin}$.

Definition 3.1. 1. α is in $Closure(\widetilde{w_0})$ if α is one of the coordinates of a solution of some Hovanski system over $\widetilde{w_0}$.

2. α is in $Closure(X)$ iff α is in $Closure(\widetilde{w_0})$ for some finite tuple $\widetilde{w_0}$ from X.

Lemma 3.1. *Closure(X) is closed under the rational operations and the primitives.*

Proof. Exercise, or see [29]. □

Theorem 3.2 *(Pfaff). α is in Closure(X) iff α is definable with parameters from X.*

Proof. The essentials of the most prominent cases are in [59,37]. □

3.3. Closure and computability

Now we revisit the argument of [37] for decidability of the restricted and unrestricted exponentials, without using Schanuel. The result is of course not decidability, but it has some computable content, and is certainly connected to observations in [52]. I focus on the Newton Approximation in [37], and cannot resist observing that a cursory search of the literature on computable analysis, prior to [10] did not turn up any discussion of Newton Approximation.

Suppose α is in Closure($\emptyset$), for one of the Pfaffian structures discussed above (these have special features, relating to computability of the primitives). Select a system $\sharp$ over $\mathbb{Q}$ so that α is a coordinate (without loss of generality the first) of a solution $\bar{x}$ of $\sharp$. Pick a solution $\bar{x}$, which is of course an isolated solution, with α the first coordinate of $\bar{x}$. Now there are many rational tuples $\bar{\theta}$ so that Newton Approximation starting at $\bar{\theta}$ converges to $\bar{x}$. I stress that I am not claiming any effectivity or uniformity in the choices made. I am rather appealing to Smale's formulation of Newton Approximation, and the idea of approximate zero, to be found in [48] and subsequent literature. The Newton Approximation involves merely iteration of certain functions analytic in a neighbourhood of $\bar{x}$ which includes $\bar{\theta}$. The crucial point is to ensure that one works in a neighbourhood where one can choose a nonzero rational lower bound for the absolute value of the Jacobian matrix, and thereby a uniform modulus of continuity for the function in the Newton Approximation and then picks the rational tuple $\bar{\theta}$ in that neighbourhood so that Smale's method works. I am not concerned here with effectivity of any choices, rather we simply pick a few rationals, and then proceed computably with the computation of the values of the Newton Approximation. Then, by remarks already in [52], the limit is computable, and so α is.

There are two things to note. Firstly, the argument relativizes. Secondly, it works for the complex exponential as well as the real cases we considered above. So, we have:

Theorem 3.3. *(For real or complex exponential, and for the various real restrictions considered above). All elements of Closure$(\widetilde{w_0})$ are computable in $\widetilde{w_0}$.*

Proof. Done. □

3.4. Prime models and computable models

It is well-known that for the various real structures (and corresponding theories) considered till now, with the exception of the "wild one", Closure$(\widetilde{w_0})$ is the prime model over $\widetilde{w_0}$ and it is in fact minimal. One can consult [55] or [32].

The computability issue in such settings is how, if X is countable, the Turing degree of the structure $Cl(X)$ relates to the Turing degree of X. This is a vague formulation, of course, but it will get sharpened as we proceed.

The notion of computable structure is by now standard [21,19]. Rabin gave a masterly foundational discussion in [41], treating some of the basic algebraic structures such as groups and fields, with special attention to factorization algorithms. The paper [21] is very congenial to me. There is a major Russian tradition going back to Malcev. By now computable model theory is a thriving subject, though it seems to me that the general computability theory has got well ahead of research on concrete algebraic issues. I will assume familiarity with the basics of computable model theory, numberings and the like, as in [21] and [41].

Schanuel's Conjecture turns out to be relevant to the issue of when the prime model (over the empty set) is computable. Note that the arguments of the preceding subsection did not involve Schanuel. However, to get computability/decidability in the area of exponentiation, it seems necessary to assume the Schanuel Condition.

Theorem 3.4. *(1) Assume SC for $\mathbb{R}$. Then the prime models of $Th(\mathbb{R}_{\exp\restriction[0,1]})$ and $Th(\mathbb{R}_{\exp})$ are computable (substructures of $\mathbb{R}$), and have the same reals.*
(2) Assume SC for $\mathbb{C}$. Then the prime models of $Th(\mathbb{R}_{\cos\restriction[0,n],\sin\restriction[0,n],n\in\omega})$, $Th(\mathbb{R}_{\exp\restriction[0,n],\cos\restriction[0,n],\sin\restriction[0,n],n\in\omega})$ and $Th(\mathbb{R}_{\exp,\cos\restriction[0,n],\sin\restriction[0,n],n\in\omega})$ are all computable, and have the same reals.

Proof. (1) This is essentially a rearrangement of the last part of the proof of [37]. Both complete theories are proved decidable, assuming Schanuel's Conjecture for $\mathbb{C}$. The theories are o-minimal, and the prime model consists of the definable elements. To such an element α we assign the least Gödel number of a formula defining it, and readily make this computable set of numbers into the prime model, computably. That the same reals are in both is seen as follows. Clearly the reals for the first theory are included in those of second, by consideration of Hovanski systems. For the other direction, take an unrestricted Hovanski system, and a solution, and by scaling write down a restricted system of which it is a solution. (2) An obvious modification of the preceding works. □

3.5. π

A very basic question is whether π is definable in $\mathbb{R}_{\exp}$ (or equivalently, by the preceding theorem) in $\mathbb{R}_{\exp\restriction[0,1]}$. It is obvious that π is definable from any of the restricted trigonometric series. It is obvious, too, that e is definable in any exponential field. The following unpublished result was obtained independently by two pairs, Macintyre–Wilkie and Van den Dries–Miller (using the results of [59] on normal form for definitions).

Theorem 3.5. *If Schanuel holds for $\mathbb{C}$ then π is not definable in $\mathbb{R}_{\exp}$.*

Proof. Exercise, using Euler and a putative Hovanski system over $\mathbb{Q}$ with π as a coordinate of a solution. □

Note that if $\frac{\pi}{e}$ is rational, then π is definable. Note also that Schanuel for $\mathbb{C}$ is a natural assumption in the above, because of the power of

$$\exp(2\pi i) = 1.$$

I illustrate by a familiar toy example. Since 1 and $2\pi i$ are linearly independent over $\mathbb{Q}$ we get:

$$\text{transcendence degree}(1, 2\pi i, \exp(1), \exp(2\pi i)) = \text{transcendence degree}(\pi, e) \geq 2.$$

I do not see how to do this without using i. I note the following.

Theorem 3.6. *The prime model over π of $Th(\mathbb{R}_{\exp})$ is computable if SC holds for $\mathbb{R}$.*

Proof. This is a simple adaptation of the method for Theorem 3.4. □

3.6. More on $\mathbb{R}_{\exp,\cos,\sin}$

The earlier discussion on this structure can be carried a little further. I do this because of a possible (undesirable) connection to $\mathbb{C}_{\exp}$.

Consider the following three categories of structures:

(1) The category of models of $Th(\mathbb{R}_{\exp,\cos,\sin})$
(2) Models of $Th(\mathbb{R}_{\mathbb{Z}})$
(3) The category of 2-sorted structures, as in [2] elementarily equivalent to the full second order theory of standard arithmetic. (Note carefully that what Apt and Marek call "second-order arithmetic" is a much weaker (axiomatic) theory.)

In each case the morphisms are model-theoretic embeddings.

In subsection 2.3 I gave the essential ingredients for pairwise interpretability at the level of the standard models. This clearly transfers to general models. These interpretations are in fact functorial (I leave it to some younger colleague to write all this out in terms of L^{eq}). This is not quite trivial. Consider, for example, how $\mathbb{Z}$ gets defined in $\mathbb{R}_{\exp,\cos,\sin}$. The definition given in subsection 2.3 is $\forall_1$, and adapts easily to $\mathbb{C}_{\exp}$. But it took ingenuity on the part of Laczkovich [33] (see later) to give a $\exists_1$ definition in $\mathbb{C}_{\exp}$. That definition adapts readily to $\mathbb{R}_{\exp,\cos,\sin}$. Again, the coding of the "power set" is seen, by inspection, to be $\forall_1$ and $\exists_1$. Coding the required analysis in $\mathbb{R}_{\mathbb{Z}}$ is easily seen to be functorial.

For me, the main point is that these functors preserve the set of reals of the structures, and this allows one to prove some negative results about the wild $\mathbb{R}_{\exp,\cos,\sin}$.

The first relevant point is a classic result [24] that shows that the sets of integers which occur in all ω-models of second-order arithmetic (this is a much weaker theory than the theory of the standard model) are exactly the hyperarithmetic sets. By our discussion of functoriality, we can transfer this to show that all hyperarithmetic reals occur in all archimedean models of $Th(\mathbb{R}_{\exp,\cos,\sin})$. Merely this observation has model-theoretic implications. In the next theorem we do not assume any Schanuel Conjecture.

Theorem 3.7. *The prime model of $Th(\mathbb{R}_{\exp})$ cannot be enriched to a model of $Th(\mathbb{R}_{\exp,\cos,\sin})$.*

Proof. Even without SC, the prime model of $Th(\mathbb{R}_{\exp})$ has only reals of degree $\leq 0'$, and so omits most hyperarithmetic reals. $\square$

In fact, the projective hierarchy [26] is involved in the definability theory of $Th(\mathbb{R}_{\exp,\cos,\sin})$. I sketch the basic folklore about this. Firstly, an open set in the reals can be coded by a real, by first construing it as a function from $\mathbb{N}$ to integers coding basic open sets with rational data. Thus, all open sets in the standard model are coded. From that it follows that all projective sets of reals are coded. The converse is clear, that sets definable using parameters are projective, using the fact that the primitives are continuous.

Thus, most definable sets are badly behaved from the standpoint of measurability, etc., in the absence of strong set-theoretic assumptions. In contrast, sets definable in $\mathbb{R}_{\exp,\cos\restriction[0,n],\sin\restriction[0,n]}$, with $n \in \omega$ are analytic, by model-completeness, and, indeed, locally closed by cell-decomposition.

There seems little point in pursuing the complexity of $Th(\mathbb{R}_{\exp,\cos,\sin})$, except for the fact that we do not know whether $\mathbb{R}$ is definable in the complex exponential field. If it is, that exponential field is deeply incomprehensible, and Zilber's Conjecture [60] extremely wrong.

I leave this topic with an observation about the prime (or minimal) model problem for $Th(\mathbb{R}_{\exp,\cos,\sin})$. In Section 6 of [2] there is a summary of the scant information known on models of the second-order theory of the standard model, due mainly to [40] and [18]. In this work it is shown that the substructure of the standard model, where the set sort consists of the sets of integers definable (without parameters!) in the standard model is the smallest model of the theory of the standard model iff the so-called analytical basis theorem holds. (The latter is true in L, by [1].) The sets definable in the standard model are exactly the analytic sets of integers. This shows that under certain set-theoretic assumptions (known to be consistent with ZFC) there can be a smallest archimedean model of $Th(\mathbb{R}_{\exp,\cos,\sin})$. Indeed, by Ellentuck [18] and our functoriality above, there can be such a model which is an elementary submodel of $\mathbb{R}_{\exp,\cos,\sin}$.

4. The complex case

4.1. $\mathbb{C}_{\exp}$

We owe to Zilber [60] the deep insight that the obvious undecidability of the complex exponential field $\mathbb{C}_{\exp}$ does not per se prevent an illuminating model theory. The conjectural model theory he presents depends on SC for $\mathbb{C}$, but there is an unconditional version for some novel exponential fields discovered by Zilber. We consider the latter in the next section, but first we concentrate on $\mathbb{C}_{\exp}$.

4.2. General setting and undecidability

K will be an exponential field of characteristic 0, with exponential E. $Ker(E)$, the additive group of periods, is

$$\{z : E(z) = 1\}.$$

For $K = \mathbb{R}$ the kernel is 0, and for $K = \mathbb{C}$ the kernel is $2\pi i\mathbb{Z}$. Tarski knew that this alone gave undecidability for $\mathbb{C}_{\exp}$, but it was only in the 1990's that Laczkovich [33] (following some remarks in [35]) proved:

Theorem 4.1. *The set of true existential sentences of* $\mathbb{C}_{\exp}$ *is undecidable. Indeed,* $\mathbb{Z}$ *is existentially definable in* $\mathbb{C}_{exp}$.

Proof. First define $\mathbb{Q}$ existentially as

$$\{z : (\exists u, v, t)[u, v \in Ker(E) \wedge zu = v \wedge tu = 1]\}$$

(the rationals are the quotients of periods).

Next we use the fact that exp is surjective to K^*, so giving us the multivalued inverse log, and the multivalued

$$z \to 2^z = \exp(z \log 2).$$

Now I claim that $\mathbb{Z}$ is

$$\{z : z \in \mathbb{Q} \wedge 2^z \in \mathbb{Q}\}. \tag{1}$$

For, pick some $\log 2$, t say (working in $\mathbb{C}$). Then any other $\log 2$ is of the form $t + 2k\pi i$ with $k \in \mathbb{Z}$. Then for any z and any $\log 2$

$$2^z = e^{z \log 2} = e^{z(t+2k\pi i)} = e^{zt} \cdot e^{2kz\pi i}.$$

Thus if $z \in \mathbb{Z}$ then $2^z = e^{zt}$, no matter which t was chosen. So any 2^z is in $\mathbb{Q}$, giving (1).

Conversely, suppose (1), and pick <u>some</u> $2^z \in \mathbb{Q}$. Say t is the corresponding $\log 2$. Now, by assumption, $z \in \mathbb{Q}$, so write $z = \frac{m}{n}$ with m and n co-prime integers. Similarly write $2^z = e^{zt} = \frac{k}{l}$ with k and l co-prime integers. Then

$$2^m = e^{tm} = e^{ztn} = (e^{zt})^n = \left(\frac{k}{l}\right)^n.$$

Then take 2-adic valuations to get that n divides m. Thus $z \in \mathbb{Z}$.

Now (1) is only an informal definition, as it involves multivalued functions. But now, after the preceding argument, it is obvious that one can define $\mathbb{Z}$ by the existential formula

$$(\exists t)[E(t) = 2 \wedge (z \in \mathbb{Q}) \wedge (E(zt) \in \mathbb{Q})]. \qquad \square$$

Note. Inspection of the argument shows that all we use about $\mathbb{C}_{exp}$ is

(1) Ker(E) has $\mathbb{Q}$-rank 1;
(2) existence of logarithms.

The most familiar condition giving (1) is

Condition 4.1 *(SP (Standard Periods)). Ker(E) is infinite cyclic.*

This is of course not a first-order condition (nor is (1)).

Note. In connection with the preceding discussion on functoriality, one should note that the proof needs only exp and a definition of $\mathbb{Q}$. Thus, it works equally well for $\mathbb{R}_{\mathrm{exp,cos,sin}}$.

Note. Laczkovich unconditionally proves the unsolvability of the decision problem for systems involving several equations. It turns out that this is inevitable, as under the assumption of SC, the decision problem for systems with a single equation is solvable. See [13] for the relevant Schanuel Nullstellensatz.

Note. It is not quite clear to me that the above analysis works for $\mathbb{R}_{cos}$. One get an existential definition of $\mathbb{Q}$ as above, but I did not push the argument further.

4.3. Defining π

This is a natural place to mention a definability result which may be startling at first sight. Recall that in the real case π is undefinable if SC holds (for $\mathbb{C}$).

Theorem 4.2. *Assume SP, existence of logarithms, and that -1 is a square. Let α and $-\alpha$ be the generators of Ker(E). Let $i^2 = -1$. Then each of $\frac{\alpha}{i}$ and $-\frac{\alpha}{i}$ is definable.*

Proof. Define

$$\cos(z) = 1/2\,(E(iz) + E(-iz))$$

and

$$\sin(z) = 1/2i\,(E(iz) - E(-iz)).$$

The graphs of cos and sin are definable in the exponential field, since the above are invariant under the permutation of i and $-i$.

It is purely formal to derive

$$\cos^2(z) + \sin^2(z) = 1$$

and the standard addition formulas.

Moreover, $\frac{\alpha}{i}$ and $-\frac{\alpha}{i}$ are periods of cos and sin. For example,

$$\cos(z + \frac{\alpha}{i}) = 1/2(E(iz + \alpha) + E(-iz - \alpha)) = 1/2(E(iz) + E(-iz)) = \cos(z).$$

Clearly, $\cos(-z) = \cos(z)$ and $\sin(-z) = -\sin(z)$.

Now, since $\mathbb{Z}$ is definable, so is the set of generators of $Ker(E)$, i.e. the set $\alpha, -\alpha$. It follows that the set $\{\frac{\alpha}{i}, -\frac{\alpha}{i}\}$ is definable, for this is the set of w such that $(\exists\lambda)\left[\lambda^2 = -1 \wedge w\lambda \in \{\alpha, -\alpha\}\right]$.

In $\mathbb{C}$, $\{\frac{\alpha}{i}, -\frac{\alpha}{i}\}$ is $\{2\pi, -2\pi\}$, and we follow this hint in a more general setting. In $\mathbb{C}$ we separate the elements of $\frac{2\pi}{4}, -\frac{2\pi}{4}$ by observing that one has $sin = 1$ and the other has $sin = -1$. Let us check the analogous observation in a more general K. Now $E(\frac{\alpha}{4})^4 = 1$, so $E(\frac{\alpha}{4})$ is a fourth root of unity. It cannot be 1 or -1 for otherwise $\alpha/4$ or $\alpha/2$ would generate $Ker(E)$. If $E(\alpha/4) = i$ then $E(-\alpha/4) = -i$, and similarly replacing i by $-i$. So, $\sin(\alpha/4i) = 1$ iff $\sin(-\alpha/4i) = -1$. So we can separate in general, and define 2π as the element of the definable $\{\frac{\alpha}{i}, -\frac{\alpha}{i}\}$ which is a zero of $\sin(z/4)$. □

Note. This does not depend on SC at all, just as Laczkovich's argument does not. However, note the essential differences between the real and complex situation as regards the definability of π.

Note. As far as I know, it is not known whether one can separate in $\mathbb{C}_{\exp}$ the two square roots of π. In contrast, a minor modification of a result in [30] shows that this cannot be done in any of Zilber's fields, so a separation in $\mathbb{C}_{\exp}$ would be dramatic.

4.4. More on "prime" models

At the level of standard, intended models we go from $\mathbb{R}_{\exp}$ to $\mathbb{C}_{\exp}$ by adjoining i and defining $\exp(iy) = \cos(y) + i\sin(y)$ for $y \in \mathbb{R}$. The problem is immediately visible, since cos and sin are not real definable from exp. The spectre of $\mathbb{R}_{\exp,\cos,\sin}$ arises. Obviously one can interpret, in a model of the theory of $\mathbb{R}_{\exp,\cos,\sin}$ a model of the theory of $\mathbb{C}_{\exp}$, but this is not illuminating. What can we say in general about starting with a model K of the theory of the real exponential and imposing on $K(i)$ an extension of the exponential field structure on K, so as to get a model of the theory of the complex exponential?

Take K as the prime model for the real exponential. We already know that if SC holds for $\mathbb{C}$ then $\pi \notin K$. (This has a clear meaning once one notes that the prime model is archimedean.) Suppose the exponential on K extends to an exponential E on $K(i)$ making this a model of $Th(\mathbb{C}_{\exp})$ satisfying SP. Let γ be the "π" of $K(i)$ in the sense of the definition just given. Let $\gamma = a + ib$, where a and b are in K. Now we define cos and sin as above. We have the usual laws, and by the discussion above $2\gamma i$ is a generator of the periods for E, and 2γ is a period for sin and cos. But we see no argument that K should be closed under cos and sin, nor that the a above is nonzero. However, if we demand that the exponential on K extend to one on $K(i)$ satisfying SC (without assuming it satisfies $Th(\mathbb{C}_{\exp})$) we can prove something (using an argument in [28]).

Theorem 4.3. *Assume SC for $\mathbb{R}_{\exp}$ Let K be the prime model of the theory of the real exponential. Then one cannot extend the exponentiation to $K(i)$ so as to satisfy SC.*

Proof. Let E be an extension of exp to $K(i)$. Fix some elements $(a_1, \dots, a_m)$ from K so that $E(i)$ is algebraic over $\mathbb{Q}(a_1, \dots, a_m)$. Since K is the prime model for $Th(\mathbb{R}_{\exp})$, one may extend $(a_1, \dots, a_m)$ to a tuple $(a_1, \dots, a_n)$ from K so that $(a_1, \dots, a_n)$ is a solution of a Hovanski system in n variables over the empty set. As usual we may assume the a_j are linearly independent over $\mathbb{Q}$, and the transcendence degree of $(a_1, \dots, a_n, E(a_1), \dots, E(a_n))$ over $\mathbb{Q}$ is n (see [37,29]), since we assumed SC for $\mathbb{R}$ and so for K. Now consider, in $K(i)$ the tuple $(a_1, \ldots, a_n, i)$. It is clearly linearly independent over $\mathbb{Q}$, but the transcendence degree of $(a_1, \ldots, a_n, i, E(a_1), \ldots, E(a_n), E(i))$ is n, contradicting SC. $\square$

Note. It is clear this can be greatly generalized, using Kirby's argument [28].

5. $\mathbb{C}$ and Zilber's fields

5.1. Summary of what is known for the complex case

Rather little is known about $Th(\mathbb{C}_{exp})$. Unconditionally its existential theory is undecidable [33], and it is not model-complete (I gave the first proof in 1991, but did not publish it. Marker [38] later gave a nicer proof, showing that $\mathbb{Q}$ is not universally definable). The existential theory has degree $0'$ by Laczkovich's proof and the Note after Theorem 2.5. But we have no bound on the complexity of the full theory, because of the dire possibility that $\mathbb{R}$ is definable. We know that the elements of the closure of the empty set consists of computable complex numbers (we do not know if this is the prime model, though that follows from Zilber's Conjecture). It then follows from [29] that:

Theorem 5.1. *SC holds for $\mathbb{C}$ iff SC holds for the exponential field of computable complex numbers.*

Proof. Kirby shows that SC holds in $\mathbb{C}_{\mathrm{exp}}$ if and only if it holds in the closure of the empty set, and from this the result is immediate. $\square$

In fact, the analogous result for the real exponential field is readily deduced from the beautiful result of [31] on uniformity in the real Schanuel Conjecture.

Note. We do not know unconditionally whether or not $Th(\mathbb{C}_{\mathrm{exp}})$ has a prime model. The results of [18] show that this will not be settled in ZFC if $\mathbb{R}$ is definable. On the other hand Zilber's Conjecture implies that there is a prime model, which is not minimal.

5.2. Basics on Zilber's fields

I recommend, apart from Zilber's already classic [60], the papers to be found on Jonathan Kirby's homepage at University of East Anglia. The essential background for what I do is the following set of facts:

1 Zilber works with the class of exponential fields of characteristic 0, satisfying SP and SC. This is not an elementary class, but readily axiomatized in $L_{\omega_1,\omega}$, where L is the natural language for exponential rings. Note that it is not quite trivial that the class is nonempty [60].
2 One uses systematically the dependence relation given by Hovanski systems (or an equivalent in more abstract Hrushovski style, as Zilber does). One isolates the category of <u>strong</u> embeddings, those where dimension of tuples does not go down. (It is useful to incorporate in the development the older notion of partial exponential field, as Kirby does.)
3 One identifies a strong notion of <u>strongly existentially closed</u> in the category of strong embeddings, and Zilber gives a beautiful "Nullstellensatz" characterizing the strongly existentially closed structures. As is customary in this kind of Robinsonian model theory. One shows that the strongly existentially closed structures are cofinal in the whole class.
4 One adds a final condition; namely, that the closure of countable sets is countable (axiomatizable in Keisler's $L(\mathbb{Q})$), and obtains startling information. Namely, the class of strongly existentially closed structures satisfying the countable closure condition has one isomorphism type for each dimension over the empty set, and so there is just one in each uncountable cardinal, and countably many types of

countable structures. It may happen that there are embeddings that are not strong, and Kirby [29] proved the nice result that embeddings are elementary (in first order sense) iff they are strong.

The essential difference between these structures and $\mathbb{C}_{\exp}$ is that they are constructed by limit procedures (heavily involving Axiom of Choice in general), while $\mathbb{C}_{\exp}$ is a visible geometric structure (and also Borel, in the sense of Borel model theory). However, Zilber has boldly conjectured that $\mathbb{C}_{\exp}$ is in the class described in (4). That it satisfies the countable closure property is clear, from separability of the topology and the isolation of zeros of Hovanski systems. That it satisfies SC is a huge assumption, not expected to be proved soon, even if it is true. But it seems reasonable to explore its consequences. This has in fact proved very worthwhile, providing new insights into Shapiro's Conjecture in complex analysis, and more generally on the zero sets of exponential polynomials over the complexes, see [14] and [15].

The remaining condition, Zilber's Nullstellensatz, has a different flavour. It happens that a few instances of it can be proved using difficult complex analysis, but it was unknown to mathematics till Zilber formulated it.

It will be convenient to refer to the structures in the above class as **strong Zilber fields**.

Among Zilber's many wonderful results is that the strong Zilber field $\mathbb{B}$ of cardinal continuum is quasi-minimal, i.e. all its definable sets are countable or cocountable, Zilber's Conjecture implies that $\mathbb{R}$ is not definable in $\mathbb{C}_{\exp}$. The reader will recall that we have described the failure of this consequence as a dire possibility.

We are going to look at computability issues for the strong Zilber fields. Note that since we have no visible metric topology on them there is no obvious notion of computable element. There is however, a definite meaning to the issue of giving a countable strong Zilber field the structure of a computable exponential field. This issue was raised by Julia Knight and me independently. Below I give a rather delicate proof that all countable strong Zilber fields are computable.

5.3. Comparisons

Laczkovich's proof gives the undecidability of the universal theory of each of the strong Zilber fields. Since his method produces an existential definition of $\mathbb{Z}$ one sees easily, both for $\mathbb{C}$ and the strong Zilber fields, that the universal theory has degree $\geq 0'$. However, I do not see how to prove the converse Turing inequality, unless I assume SC for $\mathbb{C}$, in which case one can show that the set of existential sentences true in $\mathbb{C}$ is computably enumerable, by using the decidability of exp and restricted cos and sin on $\mathbb{R}$. Thus:

Theorem 5.2. *The universal theory of the complex exponential has degree $0'$ if SC holds for $\mathbb{C}$.*

I have not been able to show directly that the same is true for the strong Zilber fields, precisely because of the lack of any filtration by distance from the origin. However, the impending construction of a computable strong Zilber field will give us the above theorem for the strong Zilber fields.

5.4. The notions involved in Zilber's Nullstellensatz

ZN, Zilber's Nullstellensatz, is a (prima facie) infinitary axiom scheme giving sufficient conditions for systems of exponential equations to be solvable "generically" in a strong extension of a field in the basic Zilber category. It turns out that this is the crucial axiom actually characterizing strong existential closure. The axiom involves a number of rather novel algebraic–geometric notions, and it is by no means obvious what is their logical, or computational, complexity. In order to look systematically at these issues, it is convenient to have to hand Kirby's papers [28,29].

The familiar first reduction is to consider only systems (over some set of parameters) whose individual equations are of the form occurring in Hovanski systems, namely

$$P(z_1, \dots, z_n, E(z_1), \dots, E(z_n)) = 0,$$

where P is a polynomial in $2n$ variables $z_1, \dots, z_n, w_1, \dots, w_n$. Now we are going to give invertible values to the w's, and so we naturally work with the product variety that P defines in $(G_a \times G_m)^n$ where G_a is affine space, and G_m is the multiplicative group. Thus we naturally consider (possibly reducible) subvarieties V of $(G_a \times G_m)^n$, and seek criteria for such V to have points $(z_1, w_1, \dots, z_n, w_n)$ on the "n-dimensional graph of E", i.e. the set $\mathcal{G}_{E,n}$ of all $(\delta_1, E(\delta_1), \dots, \delta_n, E(\delta_n))$. In fact, for the study of strong Zilber fields, we are more interested in having irreducible V and having generic points of V on $\mathcal{G}_{E,n}$. Here "generic" refers to some fixed finitely generated field over which V is defined. This will be amplified later.

As far as formulating axioms are concerned, we will (have to) deal with families of varieties indexed by some parameters, thus with $V_{\bar{\alpha}}$, as $\bar{\alpha}$ ranges over a definable set. It is classic [54] that the set of $\bar{\alpha}$ such that the subvariety $V_{\bar{\alpha}}$ of $(G_a \times G_m)^n$ is irreducible (respectively absolutely irreducible) is first-order definable. We now proceed to more delicate definability considerations. It will be convenient to drop the subscript $\bar{\alpha}$ in informal discussions.

The search for the right axiom follows long-familiar heuristics. First, look for constraints on solvability. Here we have three.

1. The functional equation for E, leading to constraints on V.
2. SP, leading to further constraints on V.
3. Schanuel's Conjecture.

In each analysis, one has already restricted to irreducible V.

In (1), one makes quite draconian restrictions on V to avoid trouble with the functional equation. One considers the following condition on a generic point $(z_1, \dots, z_n, w_1, \dots, w_n)$ of V:

(*Free of additive relations*).

This says that there is no c in K, and no rationals $(\lambda_1, \dots, \lambda_n)$, not all 0 so that

$$\text{for a generic point } (z_1, \dots, z_n, w_1, \dots, w_n) \text{ of } V, \quad \lambda_1 z_1 + \dots + \lambda_n z_n = c.$$

In (2) one does something similar, to prohibit multiplicative complications:

(*Free of multiplicative relations*)

This says that there is no d in K, and elements $(k_1, \dots, k_n)$ from $\mathbb{Z}$, not 0, so that

$$\text{for a generic point } (z_1, \dots, z_n, w_1, \dots, w_n) \text{ of } V, \quad \prod_j w_j^{k_j} = d.$$

The Schanuel Condition gives rise to a more complicated constraint, leading to a lamentable piece of notation, the use of "rotund", which I propose to abandon. To formulate the appropriate definition, let $G = (G_a \times G_m)^n$. Each $M \in M_{n\times n}$ acts on G_a additively, and on G_m multiplicatively, inducing a natural action on G, as in [60]. Write $M.V$ for the image of V under this action, and note that $M.V$ is irreducible (resp. absolutely irreducible) if V is.

Definition 5.1. V is *formally Schanuel* if V is irreducible of dimension n, and for all integer matrices M as above, of rank r strictly between 0 and n, the dimension of $M.V$ is at least r.

(One may define formally Schanuel for general V by requiring one of the components to be formally Schanuel [28,29].)

The basic nontrivial question is the status of these notions in terms of elementary definability or computation. It is important to keep track of the field K over which V is supposed to be defined. Let us assume for now that K is algebraically closed, in the formulation of constraints (1) and (2). (We will eventually have to consider the case of more general K when we start doing serious computable model theory.) Zilber [60] (Theorem 3.2) gave a very nontrivial proof of the following:

Theorem 5.3. *The condition that $V_{\bar{\alpha}}$ be free of multiplicative relations is elementary in $\bar{\alpha}$, and so quantifier-free definable.*

Similarly, he showed (also in Theorem 3.2):

Theorem 5.4. *The condition that $V_{\bar{\alpha}}$ be formally Schanuel is elementary in $\bar{\alpha}$, and so quantifier-free definable.*

Note 1. Both theorems have versions in terms of computability, if the ambient K is given effectively (of course we appeal to decidability of the theory of algebraically closed fields).

Note 2. It is important for our computable model theory to consider the case that $V_{\bar{\alpha}}$ is considered as defined over $K = \mathbb{Q}(\bar{\alpha})$, where $2\pi i$ is part of $\bar{\alpha}$, and where we have fixed a computable presentation of K. It is then uniformly computable in the $\bar{\alpha}$ whether $V_{\bar{\alpha}}$ is absolutely irreducible (because of computable quantifier elimination for algebraically closed fields). Once one knows that $V_{\bar{\alpha}}$ is absolutely irreducible, one can use the same quantifier-elimination argument to compute whether or not $V_{\bar{\alpha}}$ is free of multiplicative dependencies (resp., is formally Schanuel) with respect to K^{alg}. How to "descend" to K and check what happens there is left till later.

The situation with additive dependencies is more involved. As Kirby points out in [28,29], there is no analogue of the theorem about multiplicative relations. But there is a significant computational version, which I prove below, using Gröbner bases. I use [7] as an excellent reference.

It turns out to be easier to do the proof analysis first, and later state the theorem. The setting will be a computable field L of characteristic 0. We take a variety V as above, defined over L, and assumed absolutely irreducible. For technical reasons we work in affine space adjoining variables $t_1, \ldots, t_n$ to function as the inverses of the $w_1, \ldots, w_n$, and we adjoin the equations

$$t_j.w_j = 1. \qquad (*)$$

We work in the polynomial ring $L(z_1, \ldots, z_n, w_1, \ldots, w_n, t_1, \ldots, t_n)$, and we construe V, together with the relations (*), as an ideal $I(V)$ in this polynomial ring. A finite generating set B for this ideal is supposed given. Fix an ordering on the set of variables, with

$$z_1 < \cdots < z_n$$

being the initial segment, and compute from B a reduced Gröbner basis B^* for the original ideal, with respect to the above ordering. Note that B^* is a Gröbner basis for the ideal generated by V over the algebraic closure of L. Now we want to test if V is free (over the algebraic closure of L) of additive relations. I remind the reader that our computations have to be uniform in the parameters $\bar{\alpha}$.

The basic computational problem is:

Decide if there are $\gamma \in L$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}$, not all zero, such that

$$g = \lambda_1 z_1 + \ldots + \lambda_n z_n - \gamma \in I(V).$$

Suppose $g \in I(V)$ where the γ and $\bar{\lambda}$ are unknown. Then g gets reduced to 0 by standard reduction against the Gröbner basis B^* by the fundamental theorem of Gröbner bases. There are various cases.

Case 1 g is a constant.
Case 2 g is not a constant, and its leading nonzero term is $\lambda_j \cdot z_j$.

In the first case, test if $V(I)$ is the whole polynomial ring (using, if you like, Gröbner bases). If it is, there are additive dependencies, the set of $\lambda_1, \ldots, \lambda_n$ occurring has basis $(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1)$, and any γ in L occurs. If $V(I)$ is a proper ideal, only $\gamma = 0$ can occur, and does.

For the second case, check all the Gröbner basis elements that have z_j as leading term. These must all be linear in the variables z_l, for $l < j$. In a procedure of reduction of g to 0, we can only create linear polynomials with constant term, only linear Gröbner basis elements (with constants) can be used, and none can be used twice. Moreover a reduction step will just involve subtracting from g a constant multiple of the Gröbner basis element. So the question whether or not there is a g of the above form in $I(V)$ comes down to checking some linear algebra over L for solutions in $\mathbb{Q}$. Any reduction procedure has to use a sequence of length no more than j of linear Gröbner basis elements. Thus we see that for g of the above form $g \in I(V)$ iff there are linear elements $\Lambda_1, \ldots, \Lambda_k$ of B^* and $\delta_1, \ldots, \delta_k \in L$ so that

$$g = \sum_r \delta_r \Lambda_r.$$

The existence of such a g becomes a pure linear algebra problem about L. A crucial point is that since B^* is reduced, the δ's can be chosen in $\mathbb{Q}$. We can assume that the Λ are all the linear polynomials (maybe with constant term) occurring in B^*. With the previous notation for g the system is a system of $\leq n + 1$ linear equations in the unknowns $\lambda_1, \ldots, \lambda_n, \gamma, \delta_1, \ldots, \delta_k$, where all the unknowns except γ are from $\mathbb{Q}$, and $\gamma \in L$. There is one equation for each $1 \leq j \leq n$, and one for the constant term. The coefficients are linear combinations of the coefficients of the Gröbner basis.

To begin with, we put aside the equation corresponding to the constant term, and are left with

$$M \cdot \begin{pmatrix} \delta_1 \\ . \\ . \\ . \\ \delta_k \end{pmatrix} = t \begin{pmatrix} \lambda_1 \\ . \\ . \\ . \\ \lambda_n \end{pmatrix}$$

where M is an $n \times k$ matrix over L. We look for a solution where the δ are from $\mathbb{Q}$ and the λ are elements of $\mathbb{Q}$ not all zero. Construe M as a linear map from L^k to L^n, and the problem is to decide if the image of $\mathbb{Q}^k$ under M has nontrivial intersection with $\mathbb{Q}^n$. In fact, for other purposes we will need more, firstly to decide this, and secondly to extract computably a $\mathbb{Q}$-basis for the intersection.

This issue suggests to me imposing the following condition on a computable field K of characteristic 0.

Computable Dependence Condition.

Linear dependence over $\mathbb{Q}$ is a computable condition on finite tuples from K.

I abbreviate the condition by CDC.

Remark. There are obvious examples, such as $\mathbb{Q}(t)$ for t transcendental. I have not tried to find an example of a computable field where CDC fails, but I suppose that such exist.

Here is a first use of CDC:

Lemma 5.1. *Assume K satisfies CDC. Then there is an algorithm which produces for each $c_1, \ldots, c_k \in K$ a basis of the $\mathbb{Q}$-subspace of $\mathbb{Q}^k$ that consists of all $\lambda_1, \ldots, \lambda_k$ such that*

$$\sum_j \lambda_j c_j \in \mathbb{Q}.$$

Proof. Here is the algorithm. Let $c_1, \ldots, c_k$ be given. By applying the algorithm from the axiom to all the subsets of $\{c_1, \ldots, c_k\}$ one can compute both the dimensions of the space generated by a finite subset X of $\{c_1, \ldots, c_k\}$, and a finite subset of X which is a basis of that space. Apply this to $X = \{c_1, \ldots, c_k\}$, and go on to calculate dimension of $X \cup \{1\}$. There are two cases (each computable):

Case 1: Dimension increases, so $X \cup \{1\}$ is independent. Thus, the only rational in the space generated by X is 0. So, to find the vectors $\bar{\lambda}$ in $\mathbb{Q}^k$ whose inner product with $< c_1, \ldots, c_k >$ is rational, we have exactly to find those orthogonal to $< c_1, \ldots, c_k >$. We can assume without loss of generality that the basis of X is $< c_1, \ldots, c_l >$ for some $l \leq k$. Write

$$c_{l+r} = d_{r,1}c_1 + \ldots + d_{r,l}c_l$$

with the d's rational.

Then for $\lambda_j \in \mathbb{Q}$

$$\sum_{j=1}^{k} \lambda_j c_j = \sum_{j=1}^{l} \lambda_j{}' c_j, \quad \textit{with} \quad \lambda_j{}' = \lambda_j + \sum_{r=1}^{k-l} \lambda_{l+r} d_{r,j}$$

and so

$$\sum_{j=1}^{k} \lambda_j c_j = 0 \quad \textit{if and only if} \quad ((\forall j \leq l)(\lambda_j + \sum_{r=1}^{k-l} \lambda_{l+r} d_{r,j} = 0)$$
$$\textit{if and only if} \quad ((\forall j \leq l)(\lambda_j = -(\sum_{r=1}^{k-l} \lambda_{l+r} d_{r,j}).$$

From this it is obvious that the dimension of the set of $(\lambda_1, \ldots, \lambda_k)$ with $\sum_{j=1}^{k} \lambda_j c_j \in \mathbb{Q}$ is $k - l$, and a basis is given by the standard vectors having 0 everywhere except for a 1 at the $l + r$ place, for r running from 1 to $k - l$.

Case 2: Dimension does not extend, so there are nonzero rationals in the space generated by X. By the same kind of argument as in Case 1, we can compute a representation of 1 as a $\mathbb{Q}$-combination of elements of X, and go on to find a basis for the subspace of $\mathbb{Q}^{k+1}$ consisting of the vectors orthogonal to $< c_1, \ldots, c_k, 1 >$. □

Corollary 5.1. *Suppose K satisfies CDC. Then there is an algorithm which, given an $n \times k$ matrix M over K, provides a basis of the space of vectors $\bar{v}$ in $\mathbb{Q}^k$ such that $M\bar{v}$ is in $\mathbb{Q}^n$.*

Proof. For each row of M find a basis of the space of $\bar{v}$ in $\mathbb{Q}^k$ such that the inner product of that row with $\bar{v}$ is in $\mathbb{Q}$. Then compute (it is obvious how to) a basis for the intersection of these spaces. □

Now we apply this to the Gröbner basis problem above. We can find a basis of the set of all $\bar{v}$ in $\mathbb{Q}^r$ such that $M\bar{v}$ is in $\mathbb{Q}^j$. Thus we can decide if there is a nonzero such $\bar{v}$. If there is not, then V is free of additive dependencies. If there is one, V has additive dependencies, because once we have found the λ_j we get the constant term for free as the element you get by following out the reductions on the constant terms of the Gröbner basis. So, we have a significant result with no definability analogue.

Theorem 5.5. *For K satisfying the Computable Dependence Condition, there is an algorithm for deciding whether or not a variety V over K is free of additive dependencies.*

5.5. Constructive aspects of the relevant Kummer theory

Zilber [60] revealed a fundamental model-theoretic "stability" for his fields, via a Kummer-theoretic argument. It is of interest that this relates to a much earlier argument of Ritt [43] in the proof of his Factorization Theorem for basic exponential polynomials. Zilber's work was modified and refined by Bays and Zilber [6], and eventually, in response to a request from Bays, Gavrilovich and Hils [5] Gabber isolated a general principle valid for semi-abelian varieties (and in fact for all commutative group varieties [5]). The terminology used in the logic literature ("Thumbtack Lemma") is, once again, unappealing to me, and I will avoid it.

Here are the features crucial for my immediate purpose. One is dealing first with a finite k-tuple $\bar{\gamma}$ and the corresponding $E(\bar{\gamma})$. One is working over some partial E-field K, usually assumed to contain all roots of unity. The model-theoretic task is to figure out how E extends to the $\mathbb{Q}$-space generated by $\bar{\gamma}$. There are of course choices to be made, since all one can say immediately about $E(\frac{x}{n})$ is that is one of the finitely many nth roots of $E(x)$. Thus, one has to take account of the involvement of the Galois theory of abelian extensions of $\mathbb{Q}$ and general Kummer theory, and it is certainly not obvious that one does not have splitting of possibilities indefinitely as n increases. One wants to find the possible quantifier-free types of the $2k$-tuple $< \frac{\bar{\gamma}}{n}, E(\frac{\bar{\gamma}}{n}) >$ as n increases, in order to extend to a partial E-field containing $\bar{\gamma}$. Let V be the variety of $< \bar{\gamma}, E(\bar{\gamma}) >$. V is a subvariety of the commutative group variety $(G_a \times G_m)^k$, and the only constraint on the variety of $< \frac{\bar{\gamma}}{n}, E(\frac{\bar{\gamma}}{n}) >$ is that it is an irreducible component of $[n]^{-1}(V)$, where $[n]$ is the endomorphism of $(G_a \times G_m)^k$ which on $(G_a)^k$ is the usual multiplication by n, and on $(G_m)^k$ is exponentiation to power n. One has a projective system, indexed by the poset of divisibility, of such components, as n varies. Remarkably, for "generic" V, this profinite system is in fact finite. Note that this is a result about pullback of torsion on commutative group varieties which have finite n-torsion for every n. All I need below is the following:

Theorem 5.6. *Let $V_{\bar{\lambda}}$ be a family of subvarieties of the commutative group variety $(G_a \times G_m)^k$ over an algebraically closed K of characteristic 0. There is a bound b, computable from V such that for each $V_{\bar{\lambda}}$ which is free of both additive and multiplicative dependencies, there is an $n \le b$ so that $[m]^{-1}(V)$ is irreducible whenever n divides m.*

Proof. The condition "free" in [5] is clearly equivalent to freedom from additive and multiplicative dependencies. The existence of the bound follows from Remark 1 on their Page 8, and the computability of a bound follows from standard effectivity arguments about number of components. □

Definition 5.2. (V as above) V is Kummer-generic if $[n]^{-1}(V)$ is irreducible for every n.

Theorem 5.7. *Let $V_{\bar{\lambda}}$ be a family of subvarieties of the commutative group variety $(G_a \times G_m)^k$ over a computable algebraically closed K of characteristic 0. Then the set of $\bar{\alpha}$ for which $V_{\bar{\alpha}}$ is Kummer-generic is computable.*

Proof. This follows from the constructibility result Theorem 2.3 of [5] (extended, as they note to be possible, to general group varieties). □

6. Computable structure on countable strong Zilber fields

6.1. Refining Kirby's construction

I now give a computable version of an argument/construction in [29]. Kirby's objective is to show that for each dimension d from 0 to ω there is a unique (up to isomorphism) strong Zilber field of dimension d. My objective is to show that these exponential fields are computable.

Fix such d. Kirby proceeds by an ω-limit of ω-limit constructions, according to a standard model-theoretic procedure, meeting one requirement (for existential closure) at each stage. The delicate aspect is to meet each requirement in a canonical way, guaranteeing extension of isomorphisms, and guaranteeing omission of all relevant types. A typical local requirement is to have a variety V, assumed free of additive and multiplicative relations, and formally Schanuel, meet the multidimensional graph of exponentiation in a "generic" point. Kirby stresses the "free" aspects of such adjunctions. At every stage he work with an algebraically closed field (after the first stage it is of infinite transcendence degree). The field is usually a partial E-field.

The starting structure is the partial E-field $\mathbb{Q}^{ab}(\pi)$ of $\mathbb{C}$, the domain D of the exponential E being the $\mathbb{Q}$-space generated by $2\pi i$, and E being the analytic exponential. Note that this E-field is strongly embeddable in any Zilber field, with the π of the Zilber field mapping to the complex π. There are two possibilities, depending on identification of square roots of -1 (see [30]). The above E-field (called SK by Kirby) is certainly computable, not merely as a field, but with various important extras. Thus, SK is computable in such a way that

1. The domain and range of E are each computable subsets, and E is computable. The domain of E is given with a computable $\mathbb{Q}$-basis.
2. SK has the CDP.
3. SK satisfies a slightly sharper version of computability of freedom from additive and multiplicative dependencies (to be explained as we go along).

We are going to construct a "computable chain" of strong extensions of SK, with a computable limit. Each partial E-field arising will be a strong extension of its predecessors, and will satisfy the properties 1, 2, 3 above. The kernel will not extend, SC will be satisfied at each stage. The main task at each stage will be one of the following:

a. To adjoin algebraic elements.
b. To extend E.
c. To get logarithms.
d. To consider subvarieties V of $(G_a \times G_m)^k$, absolutely irreducible over the current field, formally Schanuel and absolutely free of dependencies, and to extend E in such a way as to meet the multidimensional graph of E in a generic point.

Kirby works systematically (as had others many years before) with partial E-fields, where LOG, the domain of E, is a $\mathbb{Q}$-subspace, and EXP, the range of E, is a divisible subgroup of the multiplicative group. He is not concerned with computability, and so has no need for various enrichments of data that I require. As mentioned already, I will need at a minimum, to have LOG and EXP computable subsets of the field in question, and I will need to have a computable basis for LOG. As regards EXP, one has the distinguished divisible torsion subgroup, consisting of the roots of unity. This should be a computable subset of the field in question. Moreover for both the divisible additive LOG and the divisible multiplicative EXP, it will be helpful to assume that one has a computable complementary subgroup, respectively $LOG^{\perp}$ and $\mathrm{EXP}^{\perp}$ giving direct decompositions of K and K^* respectively. There is nothing canonical about them. They are provided by Axiom of Choice in general situations, but they do not come for free in computable settings. Moreover, I will need to have computable bases for these complements. In the additive situation one is working with $\mathbb{Q}$-spaces. In the multiplicative one has $\mathbb{Z}$-module structure for $\frac{K^*}{Torsion(K^*)}$, making for minor variations in how I have to proceed. Remember that SK is the point of departure. There is already work involved in establishing the preceding enrichment of data for SK and its algebraic closure.

I have not been able to do these "helpful" enrichments in general, and have been forced to proceed differently. But there seems to me to be independent interest in doing the enrichment for SK, because of the nontrivial arithmetic involved.

6.1.1. The connection to heights

Let us begin with SK, the partial E-field $\mathbb{Q}^{ab}(\pi)$, with LOG = the $\mathbb{Q}$-space spanned by πi, and EXP the subgroup of roots of unity. $\mathbb{Q}^{ab}$ is of course the field got from $\mathbb{Q}$ by adjoining all roots of unity. It is obviously computable, but one should be rather more explicit about the enriched computable structure mentioned in the preceding paragraph. Thus we first represent $\mathbb{Q}^{ab}$ as the increasing union of the fields $\mathbb{L}_n$, where $\mathbb{L}_n$ is got from $\mathbb{Q}$ by adjoining μ_n, a primitive $n!$th root of unity. We imagine the μ_n chosen so that $\mu_n = {\mu_{nm}}^j$ with $j = \frac{(nm)!}{n!}$. This is of course possible, even computably. Now, $\mathbb{L}_n$ is of dimension $\phi(n!)$ over $\mathbb{Q}$ (with ϕ of course the Euler function). It has a basis consisting of the powers μ_n^k for $0 \le k \le \phi(n!)$. Given that the $n!$th cyclotomic polynomial is obtained computably from n (in any good algebra text) one thus gets computably uniformly in n a numbering of $\mathbb{L}_n$ as a computable field, with the natural inclusions as n increases being computable maps (here one uses the remark above about the choice of μ_n). This now induces, naturally, a numbering of $\mathbb{Q}^{ab}$ making it a computable field, and, moreover giving the group of roots of unity a computable subset. (We will need, computably, at a later stage, both a multiplicative complement to the group of roots of unity, and a basis for that complement.) Note that uniformly computably in n, we have $\mathbb{L}_n$ as a computable subfield of $\mathbb{Q}^{ab}$.

It is known [39] that the multiplicative group of $\mathbb{Q}^{ab}$ is free modulo the roots of unity. Thus, we know that the group of roots of unity (a divisible group) is complemented by a free abelian group, and the issue is to find, computably, such a complement and a $\mathbb{Z}$-basis for it. We do know that the quotient group has infinite rank, by considering the cosets of the standard primes. We also know that the only infinitely divisible elements are the roots of unity, because of the result in May's article. More precise information comes from considering heights, and indeed this provides the key to getting a computable basis.

We use the absolute logarithmic height h as in [11]. This is defined for all nonzero algebraic numbers, and takes non-negative real values. It takes value 0 exactly at roots of unity. Remarkably, 0 is isolated among values of h [11]. This is called the Bogomolov Property for $\mathbb{Q}^{ab}$. From this we derive a metric on $\mathbb{Q}^{ab}/EXP$ by $d(x \cdot EXP, y \cdot EXP) = h(xy^{-1})$. In this way $\mathbb{Q}^{ab}/EXP$ gets the structure of a discretely normed abelian group. Such groups are free abelian (by work of Lawrence and Zorzitto in the countable case [34,61], and Steprans [49] in general). The question is: how to extract, computably, a basis of $\mathbb{Q}^{ab}/LOG$, given the well-known obstructions to extracting bases computably in computable free modules [16]?

Bertrand's paper [8] provides, as we see below, the inductive step. But first we need a computable method for extracting a single element of a basis. By standard arguments, it suffices to find a nonzero element of the quotient group that is not an nth power for any n of absolute value bigger than 1. We use the Bogomolov Property, and can take [11] the lower bound $\frac{\log(\frac{5}{2})}{10}$ for the height of elements of $\mathbb{Q}^{ab}$ which are not zero or roots of unity. This bound is computable, though we do not use this fact. Now, if $x = y^n$ we have $h(x) = |n|h(y)$, so $h(x) \ge |n|\frac{\log(\frac{5}{2})}{10}$, giving a computable upper bound for $|n|$ in terms of $h(x)$. It is obvious that h is a computable function, say in the sense of [47]. We note of course that the values of h are in general transcendental numbers of a particularly simple kind. We do have the option of working with the exponential multiplicative version of height [11] whose values are algebraic. We know there is an element which is not an nth power for any n of absolute value bigger than 1. Here is how we find one computably.

We check through elements of $\mathbb{Q}^{ab}$ till we find an element α not a root of unity. We then find minimum polynomial f of α over $\mathbb{Q}$ (cf. [41]), of degree d say. We calculate a bound on the possible n so that α is an nth power, and we work on each possibility separately. Fix one such n, and consider the polynomial $f(x^n)$

over $\mathbb{Q}$. Factor it, computably, into irreducibles over $\mathbb{Q}$, and compute its Galois group over $\mathbb{Q}$. Consider only those for which the group is abelian. They must split in $\mathbb{Q}^{ab}$, and we find, computably, the roots. We then check if any of these roots has nth power α. If one has, f or $n > 1$, we discard α, and go on to next element of $\mathbb{Q}^{ab}$. If none has, and $n > 1$, discard N and try the others. So, computably, we reach a basis element β_0, say. Now we try to extend to a basis of $\mathbb{Q}^{ab}/EXP$, and we follow Bertrand's paper (which has estimates much finer than we need).

We proceed by an ω induction/recursion. Suppose we have defined/computed a finite sequence $\beta_1, \dots, \beta_k$ which is part of a basis of $\mathbb{Q}^{ab}/EXP$, and we want to extend by finding/computing a β_{k+1}. We know there is one, and that one will turn up in the enumeration. We do have to ensure also that the sequence of all β spans $\mathbb{Q}^{ab}/EXP$, so we should take first element γ that is not in span of the earlier β, and concentrate on getting a new β such that γ is in the span of the earlier β and the new one. But how to test that γ is not in the span of the earlier β? This means testing whether some nontrivial monomial in the earlier β and γ is a root of unity, and testing this is equivalent to testing if some nontrivial monomial is equal to 1. Once we have tested the latter (I explain how shortly), we can return to finding a basis for the integer exponent vectors giving a monomial which equals a root of unity. Only finitely many roots of unity are possible, since they must live in the field generated by the earlier β and γ. Thus the possible roots of unity can be effectively found, and we can then apply the method in [8,53] to compute a basis for possible vectors of exponents. In this way we can decide if γ is in the group generated (modulo torsion) by the earlier β. If it is not, we start to look for the new β, as explained shortly. If it is, we proceed to try the next untried γ and will eventually find one not in the span of the earlier β. So our main problem is to confront the issue of how to determine in general if there are multiplicative dependencies, and, if there are, to get a basis for the exponents giving such dependencies. We already need it in connection with γ, and we will need it also if γ has passed the test of needing a new basis element to help span it, and we have to find such a new basis element.

The general issue is how to decide if finitely many given elements are multiplicatively dependent. This is, from the standpoint of estimates and bounds, a perennial problem in diophantine geometry. (See [53] for a beautiful recent account.) The problem is:

Given algebraic numbers $\alpha_1, \dots, \alpha_m$, decide if they are multiplicatively dependent.

One does more. One finds bounds, computable from some natural data about the α, bounding the natural Euclidean norms of a basis of the group of vectors $< k_1, \dots, k_m >$ from $\mathbb{Z}^m$ such that

$$\alpha_1{}^{k_1} \dots \alpha_m{}^{k_m} = 1.$$

The more general problem of such a product being a root of unity can be reduced computably to this.

The problem has been treated by many people, and the following crude estimate more than suffices for our purposes.

Theorem 6.1. *Let $\alpha_1, \dots, \alpha_m$ be algebraic numbers not roots of unity, and d the dimension of the number field K generated by them. Let Γ be the subgroup of $\mathbb{Z}^m$ consisting of the vectors $< k_1, \dots, k_m >$ from $\mathbb{Z}^m$ such that*

$$\alpha_1{}^{k_1} \dots \alpha_m{}^{k_m} = 1.$$

Then Γ has a basis in the set of all integer vectors $\bar{v}$ of Euclidean norm less than or equal to $(h(\alpha_1) + \dots + h(\alpha_m))^k \cdot \frac{d}{c} \cdot (\frac{log(3d)}{loglog(3d))})^3$, for an absolute constant $c > 0$.

Proof. This follows easily from [8] and Theorem 4.4.1 of [11]. □

Corollary 6.1. *If K is given as a computable field algebraic over $\mathbb{Q}$, then one may compute whether or not there is any nontrivial multiplicative relation as above, and then, if there is, a basis for the group of exponents for such relations.*

Proof. Clear, since one may find computably a bound for d, using effective factorization over $\mathbb{Q}$. □

We now return to the issue of computing a basis for $\mathbb{Q}^{ab}/EXP$. So we have a finite sequence of β, and compute the first (in the computable numbering) element γ not in their span. Here is the method. Find a basis for the relations between a given γ and the β. If there is a nontrivial relation, then by purity of the group generated by the β, γ is in the span. If there is no nontrivial relation, there must be a maximal n so that γ is an n-th power modulo the subgroup generated by the β in $\mathbb{Q}^{ab}/EXP$. Thus we have to consider the following situation. Let F be the field generated by the β. We have to consider solvability in $\mathbb{Q}^{ab}$ of equations

$$y^n = (\gamma)^r \cdot \delta \cdot \mu,$$

where $n, r \in \mathbb{Z}$, δ is in the group generated by the β and μ is a root of unity. The unknown y is from $\mathbb{Q}^{ab}$. We have to bound n computably independently of δ and μ. Note that we can make a big simplification, since μ is an n-th power of another root of unity, and by absorbing this to the left hand side we can assume $\mu = 1$ as we will do now. Note that we may also assume that n is positive, by replacing y by y^{-1} if need be.

One final reduction is useful. To prove the finiteness of the set of n for which such an equation is solvable, it suffices to prove the result for powers of primes (use factorization of n into powers of primes).

Now consider the binomial polynomial

$$g(y) = y^n - (\gamma)^r \delta$$

over $F(\gamma)$.

A well-known theorem of Capelli [25] identifies very precisely when this is irreducible over $F(\gamma)$.

Case 1 n is a power of an odd prime p. Then g is irreducible over $F(\gamma)$ unless $(\gamma)^r\delta$ is a p-th power in $F(\gamma)$.

Case 2 n is a power of 2. Then either $n = 2$, and g is irreducible if and only if $(\gamma)^r.\delta$ is not a square in $F(\gamma)$, or $n > 2$ and g is irreducible if and only if $-4(\gamma)^r \cdot \delta$ is not a 4th power in $F(\gamma)$.

Suppose g is irreducible. Recall that we are interested only in g with a root in $\mathbb{Q}^{ab}$. So, we may assume that the splitting field of g has Galois group of order n, and contains all nth roots of unity. Let d be the dimension of $F(\gamma)$ over $\mathbb{Q}$. Then we have an easy absolute bound, via the Euler totient function, on the integers k such that $F(\gamma)$ contains a primitive kth root of unity. Note that we can readily compute a bound for d. By using a well known theorem of Schinzel [44] concerning irreducible binomials whose Galois group is abelian, we deduce that for n large enough (a computable bound depending on d) g is not irreducible. So now we have to analyze the small n below the computable bound, uniformly in $(\gamma)^r \cdot \delta$, and then we have to look at the general prime power n where g is reducible. The two analyses are quite different.

The case of irreducible g of small degree. We run through the finitely many possible degrees (below the computable bound). Now for each degree we need consider only finitely many g, using the same trick as above to restrict to $r < n$ and each δ a product of powers β^j for $j < n$. We can check computably which of these is irreducible over $F(\gamma)$, and discard the others. For a surviving polynomial we check (routine computable algebraic number theory) whether or not its splitting field is abelian over $\mathbb{Q}$. Again, discard those which do not have an abelian splitting field. For the survivors, we know that their roots ϵ must be in the pure hull (as always, modulo torsion) of the β, γ. Let L be the field got by adjoining these roots to $F(\gamma)$. It is now easy to see that the pure hull of β, γ, ϵ lies inside L, by repeating the preceding argument.

Now we work in L trying to identify this pure hull, which must be free by the basic result on $\mathbb{Q}^{ab}$. So the issue now is to identify the y in L which have some power in the group generated by the β, γ, ϵ and the roots of unity. First, we construct, computably, a finite set S of primes in the ring of integers of L so that all the β, γ, ϵ are S-units. Then all the y are also S-units. Now we use the generalized Dirichlet Unit Theorem. The group U of S-units is finitely generated, and the standard proof is clearly constructive in the sense that it provides computably both the torsion part and generators for the group modulo torsion. Now the group generated by the β is pure in $(\mathbb{Q}^{ab})^*/Torsion$ and so it is a summand of the group of S-units modulo torsion, and by simple linear algebra over $\mathbb{Q}$ we can assume that it is part of the chosen basis of the group of S-units modulo torsion. Now write γ in terms of the computably selected basis. γ is of the form $B \cdot (\theta_1)^{s_1} \dots (\theta_n)^{s_n}$, where B is in the group generated by the β, the θ are basis elements disjoint from the β, and the s_j are nonzero elements of $\mathbb{Z}$. The group generated by the β and the θ is a (possibly proper) summand of the S-unit group, and clearly the hull of β, γ is a subgroup of this group. We know it is free, but we have to find a basis extending the β. The argument is quite elementary. Take a typical element τ of the group generated by the β and γ. Then τ is of the form

$$\tau = B_1 \cdot ((\theta_1)^{s_1} \dots (\theta_n)^{s_n})^r,$$

where B_1 is in the group generated by the β, and $r \in \mathbb{Z}$. Now suppose y is in the hull of β, γ, so that a power $y^l = \tau$. Now y is of the form $B_2 \cdot (\theta_1)^{t_1} \dots (\theta_n)^{t_n}$, where B_2 is in group generated by the β and the $t_j \in \mathbb{Z}$. Using the basis representation, we derive the following equations:

$$lt_j = rs_j, \qquad 1 \leq j \leq n.$$

Now, we can assume without loss of generality that l and s are coprime, for we may simply remove the greatest common divisor, and get another instance of being in the hull, with smaller l. Then we conclude that l divides all the s_j, and so divides the greatest common divisor q of the s_j. Now $(\theta_1)^{s_1} \dots (\theta_n)^{s_n}$ is certainly in the hull, and so therefore is $(\theta_1)^{w_1} \dots (\theta_n)^{w_n}$, where $q.w_j = s_j$. Moreover this element, together with the β, generates γ, so to get a basis of the hull, we may replace γ by the new element, and repeat the preceding argument. Now the q is 1, and so l is 1. It follows that y is in the group generated by the β and the new element, and we may take the new element as our extra basis element for the hull. □

6.2. Completing the first step

After the hard work in getting computably a $\mathbb{Z}$-basis for $(\mathbb{Q}^{ab})^*$ modulo torsion (and observing that the torsion is complemented in this situation), we complete the effectivization of SK. We now need to extend this "complementation" to $\mathbb{Q}^{ab}(\pi)$. Note that in contrast to the requirements for LOG we need here only a $\mathbb{Z}$-module decomposition, which may be a mix of $\mathbb{Q}$ and $\mathbb{Z}$ free modules. The immediate task is to extend from $\mathbb{Q}^{ab}$ to the pure transcendental extension got by adjoining π. Note that we have already numbered $\mathbb{Q}^{ab}$, and as a limit of the numbered standard cyclotomic extensions, so our numbering comes with a computable splitting algorithm as in [41]. That we get a numbering (extending what we have) of the pure transcendental extension is obvious. We have two tasks, one for addition and one for multiplication, relating to additive and multiplicative dependence, and one about complementing LOG and EXP. To extend the complementation of EXP we simply factor rational functions of π over $\mathbb{Q}^{ab}$ into constants and irreducibles. We have unique factorization, and thus we simply extend the LOG complement by the irreducibles. Note that this automatically gives us the computability of multiplicative dependence. The additive problem is at once easier and uglier. We can test dependence over the constants (i.e. the elements of $\mathbb{Q}^{ab}$) using the Wronskian criterion, which is clearly effective, and since we already can decide $\mathbb{Q}$-dependence for constants we are done as far as computable dependence is done. For complementing LOG computably a minor variant works.

7. Computable strong Zilber fields

7.1. The goal

The goal is to construct, for each d with $0 \leq d \leq \omega$, an E-ring structure $(\omega, \oplus_d, \ominus_d, \odot_d, E_d)$ which is a strong Zilber field of dimension d, such that the E-ring operations are computable. The dimension d adds no real complication, and I will bring it back into focus only at the end of the analysis.

The rings will be constructed as direct limits of partial E-rings.

7.2. The basic constraints

The basic procedure is rather familiar. One has to realize various types in order to get E total and surjective to the units, and to get ZN satisfied. One has to omit various types to get SP and SC. The realization, in a computable setting, is a serious challenge (pace an outstanding recursion theorist), while the omission is rather routine, after Zilber's work [60].

As so often in recursive/inductive arguments, one must enrich the data, and carry along at each stage more than the requirements listed above. For example, one will have to pay careful attention to computational aspects of factorization, linear and algebraic dependence, etc. For this reason, and simply because I admire these classics, my references to computable algebra will be to the papers of Frohlich–Shepherdson [21] and Rabin [41]. It happens that Rabin's formalism is closer to the immediate needs of my work.

7.3. Numberings

As in [41], I take an indexing of a set M to be a bijection j from M to a computable subset of ω. I add:

Definition 7.1. An indexing of a family $M_n : n \in \omega$ is a bijection j from $\cup_n \{n\} \times M_n$ to a computable subset of $\omega \times \omega$, so that $j(n, x) \in \{n\} \times \omega$ for each n.

From j we obtain a (computable) family of indexings

$$j_n : M_n \to \omega$$

via $x \to j_n(x) = y$ where

$$\langle n, y \rangle = j(\langle n, x \rangle).$$

Now suppose (M, j) is an indexed set, and $X \subset M^k$, for $k \in \omega$. j^k maps M^k bijectively to the computable set $j(M)^k$, and the standard direct image functor $(j^k)_*$ gives us $(j^k)_* X \subset j(M)^k$. Those X for which $(j^k)_* X$ is computable are the basis of computable model theory. Let us call them <u>j-computable</u> (hoping that no confusion will arise).

One has from [41] the obvious notion of <u>computable map</u> between indexed sets. We need also Rabin's notion of <u>strongly computable map</u> of indexed sets: we say that

$$f : (M_1, j_1) \to (M_2, j_2)$$

is strongly computable if the image $f_* M_1$ is a j_2- computable subset of M_2.

These definitions extend (along the lines of the previous definition) to give the notion of computable map of families of indexed sets.

7.4. Computable partial E-rings

We will be considering indexed sets (M, j) together with a partial E-ring structure $(M, +, -, \cdot, E, 0, 1)$ so that $+, -, \cdot, E, 0, 1$ are j-computable, and LOG and EXP are j-computable (the latter implies that the graph of E is j-computable). It is exactly because of the conditions of LOG and EXP that Rabin's formalism suits us best.

It is convenient, for later use, to have available the family version of the above.

Definition 7.2. Suppose $\{M_n : n \in \omega\}$, together with j (giving $\{j_n : n \in \omega\}$) is an indexing. Suppose

$$\{(M_n, \oplus_n, \ominus_n, \odot_n, (LOG)_n, (EXP)_n, E_n) : n \in \omega\}$$

is a family of partial E-rings, like the individual case above. This family is called a computable family of partial E-rings if for each X from the list of primitives $+, -, \cdot, LOG, EXP$, if $X \subset M^k$ then

$$\{(n, x_1, \ldots, x_k) : (x_1, \ldots, x_j) \in (j_n^k)_* X\}$$

is computable.

The reader should see instantly the correct definitions of the various notions of a computable family of maps between members of a computable family of structures. The only one immediately relevant for me is that of a computable ω-chain of partial E-fields.

Definition 7.3. A computable ω-chain of partial E-fields is a family $\{(K_n, f_n) : n \in \omega\}$ of E-fields such that $\{K_n : n \in \omega\}$ is a computable family, each f_n is a computable morphism $K_n \to K_{n+1}$, such that with respect to the standard notation of Section 7.3

$$\{(n, x, y) : f_n(j_n^{-1}x) = j_{n+1}^{-1}y\}$$

is computable.

Notation. In this situation we write, for $n < m$,

$$f_{nm} = f_{m-1} \circ \ldots \circ f_{n+1} \circ f_n, \; \textit{and} \quad f_{nn} = 1.$$

Then in any obvious sense the f_{nm} form a computable family.

The K_n under the maps f_{nm} form a directed system. Clearly this has a direct limit K_∞, which can be represented pointwise by pairs $< m, x >$ where $x \in K_m$ but $x \notin Image(f_{nm})$ for any $n < m$. The representation of the partial E-field operations and constants, and of the limit maps $K_n \to K_\infty$ are obvious. Can K_∞ be indexed so as to make it a computable partial E-field with the limit maps uniformly computable? Here we need the assumption that the f_n are strongly computable, and then the following is a simple exercise.

Theorem 7.1. *The category of computable partial E-fields has direct limits for computable ω-chains of strongly computable morphisms, and the limit maps are strongly computable.*

7.5. Computing the field-theoretic algebraic closure

Suppose (K, j) is a computable field, with $j : K \to S$ a bijection, $j(S)$ computable. In what follows we need to obtain some embedding

$$K \xrightarrow{\lambda} K^{alg} \to S^{alg}$$

and an indexing $j^{alg} : K^{alg} \to S^{alg}$ so that λ is a strongly computable embedding. Moreover, the data for K^{alg} should be obtained computably from an index for $j(S)$ and indices for $j_*(+), j_*(-)$ and $j_*(\cdot)$.

This matter is well-known to be delicate (see [21,41]), because of issues about computable factorization over $K[x]$.

The index j induces a natural coding (or indexing) of elements of $K[x]$, and one then has the definition:

Definition 7.4. A computable field (K, j) satisfies CSA (computable splitting algorithm) if the set of (codes of) reducible $f \in K[x]$ is computable.

Note that if (K, j) has CSA, then the set of irreducibles is also computable, and one has an obvious algorithm for splitting polynomials into products of irreducibles.

We are most concerned with the situation where we have an index explicitly giving the tests for reducibility and factorization. From that index one should compute a recursive set $j(S)^{alg}$ with computable $+, -, \cdot$, and a computable map $j(S) \to j(S)^{alg}$ giving a computable extension $K \to K^{alg}$, where K^{alg} is an algebraically closed field and $K \to K^{alg}$ is algebraic. But this is precisely what Rabin does in his theorem, and he gets $K \to K^{alg}$ to be strongly computable.

The essential point is that $K \to K^{alg}$ is computed uniformly from K and a splitting algorithm for $K[x]$. Note too the triviality that K^{alg} has a computable splitting algorithm.

The step $K \to K^{alg}$ is fundamental for our construction. For each n we will reach a stage K_n, where K_n is a computable partial E-ring, and an algebraically closed field. We then do some computable (in fact strongly computable) $K_n \to K_n(\bar{\gamma})$, to meet some requirement, and we ensure $K_n(\bar{\gamma})$ has CSA, uniformly in the preceding. Then we go $K_{n+1} = K_n(\bar{\gamma})^{alg}$. That K_{n+1} is algebraically closed will be crucial for continuing the construction.

7.6. Algorithms relating to dependence and dimension

Throughout, all fields have characteristic 0. We will need to carry through all stages of a limit constructions various conditions of which CDC is a main example.

Rabin [41] starts from (an index for) a computable K, and explicitly and computably constructs a computable algebraic closure K^{alg}, with computable embedding $K \to K^{alg}$. We know that without assuming CSA for K the embedding $K \to K^{alg}$ need not be strongly computable.

If one starts with a general K and applies Rabin's elegant method, then if K has CSA, the embedding is strongly computable, and one produces computably an index for the image. Now suppose we have, for K satisfying CSA, an algorithm witnessing CDC. How to get one for K^{alg}?

It surely suffices to give the simple basic idea. Let $\lambda_1, \dots, \lambda_n$ be given in K^{alg}. First, find using CSA (see Rabin [41]) the minimum polynomials $F_1, ..., F_n$ of the $\lambda_1, \dots, \lambda_n$ over (image of) K. Now we crudely apply the primitive element theorem to find $\mu \in K^{alg}$, say of degree d over K, and $\gamma_{ij} \in K$ so that

$$\begin{aligned}
\lambda_1 &= \gamma_{10} + \gamma_{11} \cdot \mu + \gamma_{12} \cdot \mu^2 + \dots + \gamma_{1d-1} \cdot \mu^{d-1} \\
\lambda_1 &= \gamma_{20} + \gamma_{21} \cdot \mu + \gamma_{22} \cdot \mu^2 + \dots + \gamma_{2d-1} \cdot \mu^{d-1} \\
&\dots \\
\lambda_n &= \gamma_{n0} + \gamma_{n1} \cdot \mu + \gamma_{n2} \cdot \mu^2 + \dots + \gamma_{nd-1} \cdot \mu^{d-1}.
\end{aligned}$$

We argue as in Section 5.4. We have, for $c_1, \dots, c_n \in \mathbb{Q}$,

$$\sum c_j \lambda_j = 0 \Longrightarrow \sum c_j \gamma_{ji} = 0, \quad \textit{each } i$$

if and only if

$$\bar{c} \in (\gamma_{ji})^{\perp} \quad each\ i,$$

and because of CDC in K, it is (see Section 5.4) a computable condition whether the intersection is nontrivial. So we have:

Theorem 7.2. *There is an algorithm which takes one from indices of a computable field K enriched with indices for algorithms for CSA and CDC to indices of such algorithms for K^{alg}, with a strongly computable embedding $K \to K^{alg}$.*

7.7. Purely transcendental extensions

For dealing with transcendental extensions we need the following condition

Definition 7.5. K has CTC (computable transcendence condition) if the relation, on n-tuples, of being algebraically dependent over $\mathbb{Q}$ is computable, uniformly in n.

Here we start with computable K with CTC and go to $K \to K(x_1, \dots, x_n)$ where $x_1, \dots, x_n$ are algebraically independent over K.

It is well-known [21] that there is an indexing of $K(x_1, \dots, x_n)$ and a strongly computable $K \to K(x_1, \dots, x_n)$. It is also known that CSA extends uniformly computably in the sense that there is an algorithm which from data for CSA in K gives data for CSA in $K \to K(x_1, \dots, x_n)$. Here, however, we are concerned with the fate of CDC and CTC (assuming CSA is given for K).

Theorem 7.3. *CDC goes up from K to $K(x_1, \dots, x_n)$, uniformly computably.*

Proof. Clearly it suffices to exhibit an algorithm deciding if

$$F_1, \dots, F_k \in K[x_1, \dots, x_n]$$

are $\mathbb{Q}$-dependent, and this can be reduced, via consideration of coefficients, to deciding relation modules for vectors from K (see Section 5.4). □

For CTC, the problem is (it seems) more involved. We assume henceforward that $\mathbb{Q}^{alg}$ is given as a computable subset of K (this is readily arranged in our subsequently explained construction).

Here is a sketch of the main idea, which leads to a fundamental lemma used elsewhere in our proof.

Let $H_1, \dots, H_k \in K(x_1, \dots, x_n)$ be given, say as

$$H_j = F_j / G_j, \quad F_j, G_j \in K[\bar{x}].$$

Select (of course computably) the coefficients c_m $(m < M)$ of the F_j, G_j.

Decide (by assumption this is possible) whether $(c_m : m < M)$ are independent over $\mathbb{Q}$.

If yes, one has found the variety V of $(c_m : m < M)$ over $\mathbb{Q}^{alg}$, namely (0).

If no, we set about finding V. We use the fact that absolute irreducibility is, constructively, a quantifier-free condition on the coefficients of an algebraic set. Thus we start enumerating irreducible algebraic sets (in M variables) over $\mathbb{Q}^{alg}$, and testing if $(c_m : m < M)$ is on one of them.

Construe V as given by a set V of polynomials in v_m, $m < M$. Now add variables $w_1, \dots, w_n$ corresponding to the original variables $x_1, \dots, x_n$, and variables $y_1, \dots, y_k$, corresponding to the $H_1, \dots, H_k$. Each F_j, G_j

is to be construed as a word first in the c_m and the x_j, then yielding words $F_j^\sharp$, $G_j^\sharp$ by replacing all c_m by v_m. Add to V the relations

$$y_j \cdot G_j^\sharp = F_j^\sharp,$$

giving an absolutely irreducible variety $V^\sharp$ over $\mathbb{Q}^{ab}$. Our task is to find the dimension of the tuple $(y_1, \ldots, y_k)$ computed from $V^\sharp$, as the model-theoretic dimension of the projection of $V^\sharp$ onto $(y_1, \ldots, y_k)$ space, and this is well-known to be quantifier-free definable in the coefficients of $V^\sharp$ and so computable.

This completes the sketch of the proof of the following:

Theorem 7.4. *Suppose K is computable, of characteristic 0, and has $\mathbb{Q}^{alg}$ as a strongly computable subfield. Suppose K has CDC and CSA. Then so does $K(\bar{x})$, with appropriate indices uniformly computable from those in K.*

Note: The last argument is much more general, and will be used. Basically, it says that if K is computable and algebraically closed, and V is an explicitly given variety over K, then one can compute (uniformly as always) the dimension of the variety of explicitly given tuples of elements from V. We could, and perhaps should, make all this more precise in terms of schemes, but we settle for the above "naive" formulation. V is given by words on generators, and it becomes a question of computing the dimension of the set given by finitely many (rational) words on those generators. This is crucial in getting an instance of ZN satisfied computably.

7.8. Computable coherent systems of roots

As in Kirby [29], for $\alpha \in K^*$, K algebraically closed of characteristic 0, a coherent system of roots for α is a function

$$n \to \alpha^{1/n} \in K, \quad n \geq 1,$$

so that

$$(\alpha^{1/n})^n = \alpha, \quad (\alpha^{1/n_1 n_2})^{n_1} = \alpha^{1/n_2}. \tag{2}$$

We want a computable function (uniformly in computable K) $(\alpha, n) \to \alpha^{1/n}$.

If α is a power of a prime p, this is easy $\alpha^{1/p}$ = first p-th root of α, and $\alpha^{1/p^{k+1}} = (\alpha^{1/p^k})^{1/p}$, so that (2) is clear.

Now suppose that $n = n_1 \cdot n_2$ is a product of coprime proper factors. Suppose inductively that we have (2) arranged below n.

Select (computably) A, B so $An_1 + Bn_2 = 1$. Now note that <u>if</u> $\alpha^{1/n}$ can be defined to get (2), we must have

$$(\alpha^{1/n})^{n_1} = \alpha^{1/n_2}, \quad (\alpha^{1/n})^{n_2} = \alpha^{1/n_1},$$
$$\alpha^{1/n} = (\alpha^{1/n})^{An_1 + Bn_2} = (\alpha^{1/n})^{An_1} \cdot (\alpha^{1/n})^{Bn_2} = (\alpha^{1/n_2})^A \cdot (\alpha^{1/n_1})^B$$

so is unique. Let us take this "definition". Then

$$\begin{aligned}(\alpha^{1/n})^{n'} &= \alpha^{1/n_2})^{An'} \cdot (\alpha^{1/n_1})^{Bn'} = \alpha^{1/n_2})^{n_2' A n_1'} \cdot \alpha^{1/n_1})^{n_1' B n_2'} \\ &= (\alpha^{1/(n_2/n_2')})^{An_1'} \cdot (\alpha^{1/(n_1/n_1')})^{Bn_2'}.\end{aligned}$$

Now (!)

$$An'_1(\frac{n_1}{n'_1}) + Bn'_2(\frac{n_2}{n'_2}) = 1$$

so by a repeat of uniqueness argument we get

$$(\alpha^{1/n})^{n'} = \alpha^{\frac{1}{(n_1/n'_1)(n_2/n'_2)}} = \alpha^{1/(n/n')}$$

as required.

8. The construction

8.1. K_0

This is already done. Start with $\mathbb{Q}^{ab}(\pi)$ with

$$LOG = 2\pi i\mathbb{Q}$$
$$EXP = \mu = group\ of\ roots\ of\ unity$$
$$Ker = 2\pi i\mathbb{Z}$$
$$K_0 = \mathbb{Q}^{ab}(\pi)^{alg}$$

K_0 is given as a recursive partial E field, with CSA, CDC, CTC. Ker is also computable.

8.2. Dovetailing

In order to meet our dovetailing requirements later, we fix

(a) recursive enumeration of K_0
(b) recursive enumeration of (presentations of) all varieties V irreducible over K_0, and satisfying the hypotheses of ZN (these are computable, by (5.4)).

As we construct the later K_{n+1}, we will construct similar enumerations.

Now for dovetailing we use a polynomial quadrupling function $\langle\ ,\ ,\ ,\ \rangle$ (the usual one, such that $m, n, k < \langle m, n, k, l\rangle$). Use J_1, J_2, J_3, J_4 for the “projection functions”.

The basic idea is that we ensure that K_r ($r \geq 1$) satisfies

(i) if $J_4(r) \equiv 0$ (3), that the $J_1(r)$-th element of $K_{J_2(r)}$ gets in to LOG
(ii) if $J_4(r) \equiv 1$ (3), that the $J_1(r)$-th element of $K_{J_2(r)}$ gets in to EXP
(iii) if $J_4(r) \equiv 2$ (3), that the $J_1(r)$-th variety V over $K_{J_2(r)}$ satisfying hypothesis of ZN satisfies ZN.

It is evident that if we do this then K_ω the limit of the K_n's is a computable strong Zilber field.

8.3. $J_4(r) \equiv 0$ (3) – the LOG case

Here, as in all that follows, we assume that each K_s is strongly computably embedded in all later K_t.

So we find α, the $J_1(r)$-th element of $K_{J_2(r)}$, and decide if it is already in LOG (by stage K_{r-1}).

If yes, do nothing, and let $K_r = K_{r-1}$.

If not, we will make the new LOG the $\mathbb{Q}$-space generated by α and the LOG of K_{r-1}. This is computable because of CDC in K_{r-1}. Now K_r will be $K_{r-1}(x)^{alg}$, x transcendental over K_{r-1}. Getting K_r a computable field, with K_{r-1} computably embedded and with CSA, CDC, CTC, is done by the results of section 7. Section 7.8 gives a computable coherent system of roots for x, giving computable meaning to x^s, ($s \in \mathbb{Q}$), and allows E to be extended to the new LOG via

$$E(s \cdot \alpha) = x^s, \quad s \in \mathbb{Q}.$$

Moreover, the new E is computable. But it is less obvious that the new EXP is computable!

What is obvious is that we have (uniformly) a numbering of $K_r(x)$ so that the product of the old EXP and all powers x^s ($s \in \mathbb{Z}$) is computable. Moreover we have CSA, CDC, CTC for $K_r(x)$. We take this numbering and extend it in Rabin style to $K_r(x)^{alg}$, and note that by [41] this is a strongly computable map. Now let $\alpha \in K_r(x)^{alg}$, with minimum polynomial $f(y)$ over $K_r(x)$. One can of course compute f. Now suppose that α is in (the new) LOG. Then for some $m, n \in \omega$, with $(m, n) = 1$,

$$\alpha^m - \gamma \cdot x^n, \quad \gamma \in (old)LOG.$$

By [25]

$$Y^m - \gamma \cdot x^n$$

will be irreducible over $K_r(x)$ unless for some maximal prime power p^α dividing m, $Y^{p^\alpha} - \gamma \cdot x^m$ is reducible. Now Capelli's theorem applies.

If $p \neq 2$

$$Y^{p^\alpha} - \gamma \cdot x^m$$

will be irreducible over $K_r(x)$ unless $\gamma \cdot x^m$ is a p-th power in $K_r(x)$. But then x^n is a p-th power in $K_r(x)$, and so (easy exercise) $p|n$ contradicting $(m, n) = 1$.

If $p = 2$, we get the same conclusion unless $-4\gamma x^m$ is a square (we are in characteristic 0), so once more $p|mn$, contradiction.

Thus $Y^m - \gamma \cdot x^n$ is irreducible, and thus is f. Thus m, n, γ are uniquely determined, and we decide whether or not $\alpha \in$ LOG.

So we have met the ongoing requirement that LOG be computable.

8.4. $J_4(r) \equiv 1$ (3) – the EXP case

Now find α, the $J_1(r)$-th element of $K_{J_2(r)}$. If $\alpha = 0$ do nothing and let $K_r = K_{r-1}$. If $\alpha \neq 0$ decide if it is already in EXP.

If yes, do nothing and let $K_r = K_{r-1}$. Otherwise, add a new transcendental x to K_{r-1} and let $K_r = K_{r-1}(x)^{alg}$ just as in the previous section, getting CSA, CDC, CTC. Section 7.8 gives a computable coherent system α^s ($s \in \mathbb{Q}$) of roots of α. Now let LOG be the space generated by x and the old LOG, and define the new E via linearity and $E(s \cdot \alpha) = \alpha^s$.

Now LOG in computable. For we number $K_{r-1}(x)$ to get a set of linear polynomials in x over K_{r-1} to be computable, and then compute that the constant term is in the old LOG, and coefficients of x are in $\mathbb{Q}$.

Now we come to the issue of computability of EXP. This is <u>not</u> routine. Suppose $\beta \in K_r$ is given, and we want to know if β is in EXP. Now we note that inductively EXP is given at each stage computably with an explicit finite set of independent "generators" modulo torsion (here generators can be understood as

$\mathbb{Q}$-generators for EXP/Torsion). Now if $\beta \in K_r$ but not in K_{r-1} (a computable condition) then $\beta \notin$ LOG, for LOG is algebraic over the generators, which are in K_{r-1}. So we assume $\beta \in K_{r-1}$.

Now we have, computably, a basis $\lambda_1, \ldots, \lambda_r$ for the old EXP, and a basis $\lambda_1, \ldots, \lambda_r, \alpha$ for the new EXP. We have to decide if $\beta \in K_{r-1}$. We use an idea from the important paper [20].

Let $A = \mathbb{Z}[\lambda_1, \ldots, \lambda_r, \alpha, \beta] \subset K_{r-1}$, and use CSA to get computably (by a finite set of generators f) the ideal I of $\lambda_1, \ldots, \lambda_r, \alpha, \beta$ in $\mathbb{Z}[x_1, \ldots, x_{r+2}]$. First test $\mathbb{Q}$-dependence, then if positive start enumerating prime ideals of $\mathbb{Z}[\bar{X}]$ using [3], and thus find I. Now note that degree and height on $\mathbb{Z}[\bar{X}]$ are computable (into $\mathbb{R}$!). Then [20] gives a computable bound for the absolute value of exponents in one relation if there is any. Test the options. If one works, $\beta \in$ LOG. If none works, $\beta \notin$ LOG.

8.5. $J_4(r) \equiv 2$ (3) – the ZN case

Now find $V(z_1, \ldots, z_n, w_1, \ldots, w_n)$ the $J_1(r)$-th variety over $K_{J_2(r)}$ of ZN.

K_r will, *qua* field, be the algebraic closure of $K_{r-1}(V)$, the function field of V over K_{r-1}. Note that V satisfies the hypothesis of ZN over K_{r-1}. We adjoin to K_{r-1} the coordinates of a generic point $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ of V over K_{r-1}. V has dimension n over K_{r-1}. We need first to extend computably a transcendence base (over K_{r-1}) from $\{x_1, \ldots, x_n, y_1, \ldots y_n\}$.

This is done using quantifier-elimination, and dimension for definable sets in algebraically closed fields [45]. V is given explicitly using certain parameters from K_{r-1}, and, for each subset of the coordinates of a generic point, the condition that it has dimension n is equivalent to the projection of V onto the complimentary coordinates having dimension n, well-known to be elementary, and so computable. Thus we find a transcendence base

$$\{x_j : j \in E_1\} \cup \{y_k : k \in E_2\}$$

where E_1 and E_2 are subsets of $\{1, \ldots, n\}$, whose cardinalities have sum n. Fix one such base, and call it B.

By similar methods, one gets computably for each element of

$$\{x_j : j \notin E_1\} \cup \{y_k : k \notin E_2\}$$

a minimum polynomial over $K_{r-1}(B)$ (use CSA for $K_{r-1}(B)$).

Now construct $K_{r-1}(B)^{alg}$ with $K_{r-1}(B)$ computably embedded.

Now we take the new LOG to be $\mathbb{Q}$-space spanned by old LOG and the x_j's. By freedom from additive dependencies, this is free on the (canonical) generators of the old LOG and the x_j's. By CDC in K_r, this is computable.

The new EXP will be the divisible closure of the old EXP and the y_k's. By the Evertse–Györy method, this is computable.

How to define E computably? Here we have the standard problem of coherent choice of m-th roots for all n, and the phenomenon of Kummer genericity [5] comes into the picture.

Obviously, we will define $E(x_j) = y_j$, and extend by additivity. This puts a part of the multidimensional graph of E on the variety V. The problem is how to extend coherently, following some recipe

$$\text{“}E\left(\frac{1}{k}x_j\right) = y_j^{\frac{1}{k}}\text{”}.$$

It seems there are two ways to deal with this. One is to use the multiplicative independence of the y_j's over K_{r-1}, plus computable coherent systems of roots, to get a computable E.

The other, deeper, and consequently more fruitful for further developments, is to use Kummer genericity.

Consider, for each j, the map $[j] : \mathbb{A} \times G_m$ given by multiplication by j in $\mathbb{A}$, and exponentiation to power j in G_m. We write $[j]$ also for $[j] \times \ldots \times [j]$ n times.

Now consider the various $[j]^{-1}V$. Some may be reducible. Note that we have a projective system, indexed by divisibility, since $[j_1] \circ [j_2] = [j_1 j_2]$. In other words,

$$[j_1 j_2]^{-1}V = [j_1]^{-1}([j_2]^{-1}V).$$

Now the big result is that uniformly in families of such V, there is a computable m_0 such that $[dm_0]^{-1}V$ is irreducible, for all d.

Now note that it is computable in m and V whether or not $[m]^{-1}V$ is irreducible, so it is computable in V to find m_0.

Note that each $[k]$ is finite-to-one. It follows easily that <u>any</u> point of $[dm_0]^{-1}(\bar{x}, \bar{y})$ is a generic point of $[dm_0]^{-1}V$ (over K_{r-1}). Thus we can give a coherent meaning to $(\bar{y})^{1/dm_0}$ by selecting the point so

$$\left(\frac{1}{dm_0}\bar{x}, (\bar{y})^{\frac{1}{dm_0}}\right)$$

has least index in $[dm_0]^{-1}(\bar{x}, \bar{y})$. Finally $\bar{y}^{1/d}$ can be $\left((\bar{y})^{\frac{1}{dm_0}}\right)^{m_0}$. Thus we define E computably.

It is now obvious that K_ω is a computable model of Zilber's axioms. What is the (Zilber) dimension of K_ω?

Theorem 8.1. *The K_ω just constructed has dimension* 0.

Proof. Clearly every element of K_0 has dimension 0, as π is a transcendence base and π has dimension 0 [60,30]. Suppose that we assume inductively that each element of K_{-1} has dimension 0. At stages $J_1(r) \equiv 0$ (3) we add a new element α (from K_{r-1}) LOG, via adjoining a transcendental y with $E(\alpha) = y$. Thus y has dimension 0, and since it is a transcendence base for K_r over K_{r-1} we are done. The argument for $J_1(r) \equiv 1$ (3) is similar. For $J_1(r) \equiv 2$ (3) we need a more difficult argument. But there we adjoin a tuple $(x_1, \ldots, x_n, y_1, \ldots, y_n)$, a generic (algebraic dimension n) point of V (an instance of ZN), and put $E(x_j) = y_j$. Now $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ is a nonsingular point of V by genericity, and by the differential equation for E it follows that $V(x_1, \ldots, x_n, E(x_1), \ldots, E(x_n))$ gives a Hovanski system over K_{r-1}, when $x_1, \ldots, x_n, y_1, \ldots, y_n$ are all of dimension 0, whence the result. □

8.5.1. How to get higher dimension?

How to get dimension d, $1 \leq d \leq \omega$? One basically must adjoin, over the K_0 we used above, a set $\{t_j : 1 \leq j \leq d\}$ of exponentially independent t_j's, and later do everything else exponentially algebraic over the t_j's, without introducing any exponential–algebraic dependence between the t_j's.

All becomes clear if one shows that all the $K_r \to K_{r+1}$ are strong embeddings of partial E-rings. This kind of verification is done by Zilber and Kirby [29] in a setting not constrained by computability considerations.

Because of our explicit attention to the construction of LOG_r and EXP_r, it is firstly easy to verify that each $K_{r-1} \to K_r$ is a <u>strong</u> embedding of partial E-fields.

Let us use Kirby's definition of <u>strong</u> (Definition 2.2 in [29]).

To show that each $K_{r-1} \to K_r$ is strong we have to show exactly that if $\bar{x}$ is a tuple from LOG_r then

$$trans\ deg_{\mathbb{Q}}(\bar{x}, \overline{E(x)} \mid LOG_{r-1}, EXP_{r-1}) \geq lin\ dim_{\mathbb{Q}}(\bar{x} \mid LOG_{r-1}). \tag{3}$$

We deal with the three cases $J_4(r) \equiv m$ (3), $0 \leq m \leq 2$, separately.

Case 0 $J_4(r) \equiv 0$ (3)

There is a trivial subcase $\mathrm{LOG}_r = \mathrm{LOG}_{r-1}$, when (3) is trivial.

Otherwise, there is a $\alpha \in K_{r-1}$,

$$LOG_r = LOG_{r-1} \oplus \mathbb{Q} \cdot \alpha,$$

and $E(\alpha)$ is transcendental over K_{r-1}. Now let $\bar{x}$ be as in (3). Let $\langle \bar{x} \rangle_{\mathbb{Q}}$ be the $\mathbb{Q}$-sphere generated by the entries of $\bar{x}$. If $\langle \bar{x} \rangle_{\mathbb{Q}} \subset LOG_{r-1}$, then the right-hand side of (3) is 0, and the left-hand side is 0, so (3) holds. If, however, $\langle \bar{x} \rangle_{\mathbb{Q}} \not\subset LOG_{r-1}$ then $\langle \overline{E(x)} \rangle$ has transcendence degree 1 over K_{r-1}, $\langle \bar{x} \rangle_{\mathbb{Q}} + LOG_{r-1}$ has dimension equal to $1 + LOG_{r-1}$, so again (3) holds.

Case 1 $J_4(r) \equiv 1$ (3)

Again there can be a trivial case $\mathrm{LOG}_r = \mathrm{LOG}_{r-1}$.

Otherwise, we have $\alpha \neq 0$ in K_{r-1}, not in LOG_{r-1}, and we add a transcendental y to K_{r-1}, giving $K_r = (k_{r-1}(y))^{alg}$,

$$LOG_r = LOG_{r-1} \oplus \mathbb{Q} \cdot y, \quad E(y) = \alpha$$

and so on.

This time, if $\langle \bar{x} \rangle_{\mathbb{Q}} \subset LOG_{r-1}$, then the right-hand side of (3) is 0, and the left-hand side is 0 also.

If, however, $\langle \bar{x} \rangle_{\mathbb{Q}} \not\subset LOG_{r-1}$ then the transcendence degree of $\bar{x}$ over K_{r-1} is at least 1 because of y. Thus again (3) holds.

Case 2 $J_4(r) \equiv 2$ (3)

Again there can be a trivial case $\mathrm{LOG}_r = \mathrm{LOG}_{r-1}$.

Otherwise we have a variety $V(u_1, \dots, u_n, v_1, \dots, v_n)$ satisfying hypotheses of ZN on K_{r-1} and we adjoin coordinates of a generic point $(u_1, \dots, u_n, v_1, \dots, v_n)$ and have

$$LOG_r = LOG_{r-1} \oplus \mathbb{Q}u_1 \oplus \dots \oplus \mathbb{Q}u_n, \quad E(u_j) = v_j,\ 1 \leq j \leq n.$$

As before, if $\langle \bar{x} \rangle_{\mathbb{Q}} \subset LOG_{r-1}$, then the right-hand side of (3) is 0, and the left-hand side is 0 also. If, however, $\langle \bar{x} \rangle_{\mathbb{Q}} \not\subset LOG_{r-1}$ then suppose

$$\langle \bar{x} \rangle_{\mathbb{Q}} / (\langle \bar{x} \rangle_{\mathbb{Q}} \cap LOG_{r-1})$$

has $\mathbb{Q}$-dimension d. Then the right-hand side of (3) is d. But since V is formally Schanuel, it follows that the left-hand side of (3) is $\geq d$. Thus we have proved the following.

Theorem 8.2. *Each $K_{r-1} \to K_r$ is strong.*

Note/Recall A partial E-field K satisfies SC if it is a strong extension of K_0 $(= (SK)^{alg}$, in Kirby notation).

So (if it was not already clear) gives that K_ω satisfies SC. It is easy to show that K_ω satisfies SP (see [29]).

Finally the way is open for the general result.

Theorem 8.3. *For each d with $0 \leq d \leq \omega$, there is a computable strong Zilber field of dimension d.*

Proof. We already have the result for $d = 0$. Fix a computable strong Zilber field L_0 of dimension 0. Now take algebraically independent $\bar{c} = \{c_j : j < d\}$ and first form the partial E-ring $L_0[\bar{c}]$, with $\mathrm{LOG} = L_0$, $\mathrm{EXP} = L_0^*$. Now form $L_0[\bar{c}]^E$ the free E-ring of exponential power series in the $\bar{c}$ over L_0 [13]. This is clearly a computable partial E-ring, with L_0 computably embedded. Now pass to the field of fraction $L_{1/2}$. Do not extend LOG or EXP. The well-known argument that $L_0[\bar{c}]^E$ satisfies SC since L_0 does, shows that $\bar{c}$ is independent with respect to the dimension [60] coming from the standard pre-dimension δ.

It is obvious that $L_0[\bar{c}]^E$, and then $L_{1/2}$ is computable with CSA, so one may go (without extending LOG or EXP) to $L_1 = (L_{1/2})^{alg}$. Thereafter one goes through

$$L_0 \to L_1 \to L_2 \to \dots$$

a computable chain with limit L_∞, a computable strong Zilber field, using a dovetailing, and the three basic manoeuvres, as in the dimension 0 case. It is clear that L_∞ is E-algebraic over $\bar{c}$ (cf. the argument in the dimension 0 case). The preceding result about strong embeddings shows that $\bar{c}$ is independent in L_∞, which is a strong extension of L_1. $\square$

References

[1] John Addison, Some consequences of the axiom of constructibility, Fund. Math. 46 (3) (1959) 337–357.
[2] Krzysztof R. Apt, Wiktor Marek, Second order arithmetic and related topics, Ann. Math. Logic 6 (3) (1974) 177–229.
[3] Matthias Aschenbrenner, Ideal membership in polynomial rings over the integers, J. Amer. Math. Soc. 17 (2) (2004) 407–441.
[4] Jeremy Avigad, Vasco Brattka, Computability and Analysis: The Legacy of Alan Turing, Turing's Legacy, Cambridge University Press, Cambridge, UK, 2012.
[5] Martin Bays, Misha Gavrilovich, Martin Hils, Some definability results in abstract Kummer theory, Int. Math. Res. Not. IMRN rnt057 (2013), 26 pages.
[6] Martin Bays, Boris Zilber, Covers of multiplicative groups of algebraically closed fields of arbitrary characteristic, Bull. Lond. Math. Soc. 43 (4) (2011) 689–702.
[7] Thomas Becker, Volker Weispfenning, Gröbner Bases, Springer, 1993.
[8] Daniel Bertrand, Duality on tori and multiplicative dependence relations, J. Aust. Math. Soc. A 62 (02) (1997) 198–216.
[9] Ricardo Bianconi, Nondefinability results for expansions of the field of real numbers by the exponential function and by the restricted sine function, J. Symbolic Logic 62 (04) (1997) 1173–1178.
[10] Lenore Blum, Mike Shub, Steve Smale, et al., On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines, Bull. Amer. Math. Soc. (N.S.) 21 (1) (1989) 1–46.
[11] Enrico Bombieri, Walter Gubler, Heights in Diophantine Geometry, vol. 4, Cambridge University Press, 2007.
[12] B.F. Caviness, M.J. Prelle, A note on algebraic independence of logarithmic and exponential constants, ACM SIGSAM Bull. 12 (2) (1978) 18–20.
[13] Paola D'Aquino, Angus Macintyre, Giuseppina Terzo, Schanuel nullstellensatz for Zilber fields, Fund. Math. 207 (2) (2010) 122–143.
[14] Paola D'Aquino, Angus Macintyre, Giuseppina Terzo, From Schanuel's conjecture to Shapiro's conjecture, Comment. Math. Helv. 89 (3) (2014) 597–616.
[15] Paola D'Aquino, Angus Macintyre, Giuseppina Terzo, Comparing $\mathbb{C}$ and Zilber exponential fields: zero sets of exponential polynomials, J. Inst. Math. Jussieu 15 (1) (2016) 71–84.
[16] Rodney G. Downey, Denis R. Hirschfeldt, Asher M. Kach, Steffen Lempp, Joseph R. Mileti, Antonio Montalbán, Subspaces of computable vector spaces, J. Algebra 314 (2) (2007) 888–894.
[17] Lou van den Dries, On the elementary theory of restricted elementary functions, J. Symbolic Logic 53 (3) (1988) 796–808.
[18] Erik Ellentuck, A minimal model for strong analysis, Fund. Math. 73 (1971) 125–131.
[19] Yuri L. Ershov, Sergei Goncharov, Anil Nerode, Jeff Remmel, Handbook of Recursive Mathematics, North-Holland, 1998.
[20] Jan-Hendrik Evertse, Kálmán Győry, Effective results for unit equations over finitely generated integral domains, in: Mathematical Proceedings of the Cambridge Philosophical Society, vol. 154, Cambridge University Press, 2013, pp. 351–380.
[21] Albrecht Frohlich, John C. Shepherdson, Effective procedures in field theory, Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. 248 (950) (1956) 407–432.
[22] Andrei Gabrièlov, Projections of semi-analytic sets, Funct. Anal. Appl. 2 (4) (1968) 282–291.
[23] Guido Gherardi, Alan Turing and the foundations of computable analysis, Bull. Symbolic Logic 17 (03) (2011) 394–430.
[24] Andrzej Grzegorczyk, Andrzej Mostowski, Czeslaw Ryll-Nardzewski, The classical and the ω-complete arithmetic, J. Symbolic Logic 23 (02) (1958) 188–206.
[25] Irving Kaplansky, Fields and Rings, University of Chicago Press, 1972.
[26] Alexander S. Kechris, Classical Descriptive Set Theory, vol. 156, Springer-Verlag, New York, 1995.
[27] Askold G. Khovanskiĭ, Fewnomials, vol. 88, American Mathematical Society, 1991.
[28] Jonathan Kirby, Exponential algebraicity in exponential fields, Bull. Lond. Math. Soc. 42 (5) (2010) 879–890.
[29] Jonathan Kirby, Finitely presented exponential fields, Algebra and Number Theory 7 (4) (2013) 943–980.
[30] Jonathan Kirby, Angus Macintyre, Alf Onshuus, The algebraic numbers definable in various exponential fields, J. Inst. Math. Jussieu 11 (04) (2012) 825–834.
[31] Jonathan Kirby, Boris Zilber, The uniform Schanuel conjecture over the real numbers, Bull. Lond. Math. Soc. 38 (4) (2006) 568–570.
[32] Julia F. Knight, Anand Pillay, Charles Steinhorn, Definable sets in ordered structures, II, Trans. Amer. Math. Soc. 295 (2) (1986) 593–605.

[33] Miklós Laczkovich, The removal of π from some undecidable problems involving elementary functions, Proc. Amer. Math. Soc. 131 (7) (2003) 2235–2240.
[34] John Lawrence, Countable abelian groups with a discrete norm are free, Proc. Amer. Math. Soc. 90 (3) (1984) 352–354.
[35] Angus Macintyre, Schanuel's conjecture and free exponential rings, Ann. Pure Appl. Logic 51 (3) (1991) 241–246.
[36] Angus Macintyre, Exponential Algebra, Lecture Notes in Pure and Applied Mathematics, 1996, pp. 191–210.
[37] Angus Macintyre, Alex J. Wilkie, On the decidability of the real exponential field, in: P. Odifreddi (Ed.), Kreiseliana, A.K. Peters, 1996.
[38] David Marker, A remark on Zilber's pseudoexponentiation, J. Symbolic Logic 71 (3) (2006) 791–798.
[39] Warren May, Fields with free multiplicative groups modulo torsion, Rocky Mt. J. Math. 10 (3) (1980) 599–604.
[40] Andrzej Mostowski, Partial orderings of the family of ω-models, Stud. Logic Found. Math. 74 (1973) 13–28.
[41] Michael O. Rabin, Computable algebra, general theory and theory of computable fields, Trans. Amer. Math. Soc. 95 (1960) 341–360.
[42] Jean-Pierre Ressayre, Integer parts of real closed exponential fields, in: P. Clote, J. Krajicek (Eds.), Arithmetic, Proof Theory and Computational Complexity, Oxford University Press, New York, 1993.
[43] Joseph F. Ritt, A factorization theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i x}$, Trans. Amer. Math. Soc. 29 (3) (1927) 584–596.
[44] Andrzej Schinzel, Polynomials with Special Regard to Reducibility, vol. 77, Cambridge University Press, 2000.
[45] Philip Scowcroft, Lou van den Dries, On the structure of semialgebraic sets over p-adic fields, J. Symbolic Logic 53 (04) (1988) 1138–1164.
[46] John Shackell, The exponential identity problem and the Schanuel conjecture, Technical report, University of Kent, 1986.
[47] Stephen G. Simpson, Subsystems of Second Order Arithmetic, vol. 1, Cambridge University Press, 2009.
[48] Steve Smale, Newton's Method Estimates from Data at One Point, Springer, 1986.
[49] Juris Steprāns, A characterization of free abelian groups, Proc. Amer. Math. Soc. 93 (1985) 347–349.
[50] Alan M. Turing, Equivalence of left and right almost periodicity, J. Lond. Math. Soc. (2) 1 (4) (1935) 284–285.
[51] Alan M. Turing, On computable numbers, with an application to the entscheidungsproblem, J. Math. 58 (1936) 345–363.
[52] Alan M. Turing, Finite approximations to Lie groups, Ann. of Math. (2) 39 (1938) 105–111.
[53] Jeffrey Vaaler, Heights on groups and small multiplicative dependencies, Trans. Amer. Math. Soc. 366 (6) (2014) 3295–3323.
[54] Lou van den Dries, Exponential rings, exponential polynomials and exponential functions, Pacific J. Math. 113 (1) (1984) 51–66.
[55] Lou Van den Dries, Tame Topology and O-Minimal Structures, vol. 248, Cambridge University Press, 1998.
[56] Lou van den Dries, Angus Macintyre, David Marker, The elementary theory of restricted analytic fields with exponentiation, Ann. of Math. (2) 140 (1994) 183–205.
[57] Lou Van den Dries, Chris Miller, Geometric categories and o-minimal structures, Duke Math. J. 84 (2) (1996) 497–540.
[58] Alex J. Wilkie, On the theory of the real exponential field, Illinois J. Math. 33 (1989) 384–408.
[59] Alex J. Wilkie, Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function, J. Amer. Math. Soc. 33 (1996) 1051–1094.
[60] Boris Zilber, Pseudo-exponentiation on algebraically closed fields of characteristic zero, Ann. Pure Appl. Logic 132 (1) (2005) 67–95.
[61] Frank Zorzitto, Discretely normed abelian groups, Aequationes Math. 29 (1) (1985) 172–174.