On the complex exponentiation restricted to the integers

Carlo Toffalori, Kathryn Vozoris[1]

Department of Mathematics and Computer Science
University of Camerino
Via Madonna delle Carceri 9, 62032 Camerino, Italy

{carlo.toffalori, kathryn.vozoris}@unicam.it

Keywords. Complex exponentiation, Quasi minimality, Tarski-Vaught Test.

Abstract. We provide a first order axiomatization of the expansion of the complex field by the exponential function restricted to the subring of integers modulo the first order theory of $(\mathbf{Z}, +, \cdot)$.

2000 Mathematics Subject Classification: 03C60

1 Introduction

Let $(\mathbf{C}, +, -, \cdot, 0, 1)$ ($\mathbf{C}$ for short) be the complex field, a typical strongly minimal structure. Let $\mathbf{C}_{exp}$ denote its expansion by the exponential function $exp : z \to e^z$. It is known that the model theory of $\mathbf{C}_{exp}$ is not as well established or developed as that of its companion structure $\mathbf{R}_{exp}$. In fact the ring of integers can be defined in $\mathbf{C}_{exp}$, and consequently $\mathbf{C}_{exp}$ inherits all the complexity of the first order theory of $(\mathbf{Z}, +, \cdot)$. Also, one can see that the theory of $\mathbf{C}_{exp}$, unlike that of $\mathbf{R}_{exp}$ [6], is not model complete. There are several open questions regarding $\mathbf{C}_{exp}$: among them whether $\mathbf{C}_{exp}$ is quasi minimal (meaning that every definable subset is either countable or co-countable), in particular whether $\mathbf{R}$ is definable in $\mathbf{C}_{exp}$.
Despite these obstructions, Zilber has developed a nice approach to $\mathbf{C}_{exp}$ in [7], singling out an $L_{\omega_1,\omega}(Q)$-sentence Φ (where Q is the quantifier *"there are uncountably many"*) on algebraically closed exponential fields such that Φ admits a unique model of power λ for every uncountable cardinal λ up to isomorphism. However it remains unknown whether $\mathbf{C}_{exp}$ is really the only model of power $2^{\aleph_0}$ of Φ.
In her PhD Thesis [5] the second author dealt with $(\mathbf{C}, \mathbf{Z})$ –a structure definable in $\mathbf{C}_{exp}$, that also inherits the negative features of the ring of integers. But [5] points out that $(\mathbf{C}, \mathbf{Z})$ is quasi minimal and its first order theory eliminates quantifiers up to quantification over the integers. This adapts the result

[1]Work supported by a Postdoctoral Fellowship (2008) of the Marie Curie Research Training Network in Model Theory and its Applications MODNET, MRTN-CT-2004-512234.

of Casanovas and Ziegler [1] valid for all the strongly minimal structures expanded by a unary predicate, to the setting of (**C**, **Z**), greatly simplifying the analysis of definable sets in the structure. Also, [5] examines the complexity of (**C**, **Z**) by "forgetting" the definable sets generated by the integers and using a Morley rank modulo a predicate PMR (as defined in [2]). Observe that under the model theoretic point of view expanding the complex field by either the ring of integers or its field of fractions –that is, the field of rationals– makes no substantial difference, as the two structures, **Z** and **Q** are biinterpretable in **C**.
The aim of this paper is to pursue the approach in [5]. In fact, we deal with the structure (**C**, **Z**, exp) where

- **C** is, as said, the field of complex numbers,
- **Z** is the subring of integers,
- exp is the exponential function $z \mapsto e^z$ restricted to **Z**.

More generally we consider exponentiation with respect to any basis $\epsilon \neq 0$ in **C**, viewed as a function exp_ϵ from **Z** to **C**; so, in this larger perspective, exp as described before is just exp_e. Of course the value of $\epsilon = exp_\epsilon(1)$ can be altered, which will affect the analysis of (**C**, **Z**, exp_ϵ). We will discuss in the next section all such possible cases.
Let L denote the language of these structures (**C**, **Z**, exp_ϵ), that is L expands the language of fields by a unary relation symbol Z for **Z** and a unary operation symbol EXP for exp_ϵ (formally speaking, exp_ϵ in this setting is only a partial function, but can easily be enlarged to the whole domain in some artificial way).
Let us introduce some further notation. We refer here to L-structures $\mathcal{C}$ expanding an algebraically closed field C of characteristic 0 such that $Z(\mathcal{C})$ is a model of the first order theory of the ring of integers. Then

- $Q(\mathcal{C})$ is the field of fractions of $Z(\mathcal{C})$;
- $E(\mathcal{C})$ denotes the ring generated by the union of $Z(\mathcal{C})$ and its image in EXP;
- $K(\mathcal{C})$ is the field of fractions of $E(\mathcal{C})$, so the subfield generated by the union of $Z(\mathcal{C})$ and its image under EXP.

Observe that $Q(\mathcal{C})$ is definable in $\mathcal{C}$; but, as we will see later, $E(\mathcal{C})$ and $K(\mathcal{C})$ are not. When $\mathcal{C} = (\mathbf{C}, \mathbf{Z}, exp)$, then $Q(\mathcal{C})$ is the field of rationals, $E(\mathcal{C}) = \mathbf{Z}[\epsilon, \epsilon^{-1}]$ and $K(\mathcal{C}) = \mathbf{Q}(\epsilon)$.
Here is a brief outline of the paper. In the next section we will distinguish our analysis according to whether ϵ is algebraic or transcendental. In particular we will show that ϵ is algebraic if and only if exp_ϵ is definable in (**C**, **Z**). Of course our main focus is on the transcendental case, and indeed without loss of generality on $\epsilon = e$, therefore on exp. Hence in § 3 we will describe and discuss several consequences of the transcendence assumption, which will lead in § 4 to a tentative axiomatization T of the first order theory of (**C**, **Z**, exp). Finally, we will prove in § 5 that T is complete, whence it really equals the theory of

(**C**, **Z**, exp). Not surprisingly, a Schanuel property – stating that if $M_1, ..., M_k$ are non standard integers and $1, M_1, ..., M_k$ are linearly independent over the standard rationals, then $EXP(1), EXP(M_1), \dots, EXP(M_k)$ are algebraically independent over $Q(\mathcal{C})$– plays a crucial role in this axiomatization. See [4] for a general discussion of the relevance of this kind of property to the model theory of exponentiation.
We refer to [3] for basic model theoretic results. We heartily thank Jonathan Kirby for his attention to a previous version of these notes. His suggestions and comments greatly improved it.

2 The definability of exp_ϵ

In this section we work in the complex field **C** with a 1-ary predicate Z for the integers and a 1-ary function symbol EXP for exp_ϵ – viewed as a group homomorphism from the additive group of integers to the multiplicative group of non-zero complex numbers. As said ϵ is the image of 1 under this morphism. Its value clearly affects the analysis of the resulting structure. Actually, as (**Z**, $+$) is cyclic, the isomorphism class of (**C**, **Z**, exp_ϵ) is fully determined by the algebraic type of ϵ. For instance, when $\epsilon = 1$, exp_ϵ is constant. Also $\epsilon = -1$ is trivial to treat. We consider the following less "simple" cases.

Example 2.1 Assume that ϵ is an integer ≥ 2. Observe that ϵ is in the definable closure of the ring of integers, and hence of (**C**, **Z**). Also, recall that

(i) by Lagrange's Theorem, the set **N** of natural numbers with its addition and multiplication is $\emptyset$-definable in the ring of integers,

(ii) the function taking any ordered pair (x, y) of natural numbers to x^y (and to 1 when $x = y = 0$) is recursive, and consequently arithmetical, that is, $\emptyset$-definable in (**N**, $+$, $\cdot$).

It turns out that in this case our structure is $\emptyset$-definable in (**C**, **Z**). Moreover E defines the subring generated by ϵ^{-1} and K the field of rationals. Similar conclusions can be obtained when ϵ is a negative integer ≤ -2 and even when ϵ is rational.

Assume now that ϵ is algebraic (but not a rational). Then E defines $\mathbf{Z}[\epsilon, \epsilon^{-1}]$ while K determines $\mathbf{Q}(\epsilon)$. Some particular subcases are very easy to handle.

Example 2.2 Suppose that ϵ is a root of 1, say a primitive t-th root for some integer $t \geq 2$. Then, for every natural n, $exp_\epsilon(n) = \epsilon^r$ where r is the remainder of n divided by t, hence exp_ϵ is first order definable in (**C**, **Z**) by the formula saying that for some natural $r < t$ r is just the remainder of n divided by t and $exp_\epsilon(n)$ is the product of r factors equal to ϵ.
The case in which ϵ is the root of a rational number α, can be managed in a similar way. Assume $\epsilon^t = \alpha$ where t is an integer ≥ 2 and the polynomial $x^t - \alpha$ is irreducible over **Q**. Then the powers of ϵ are of the form $\epsilon^r \cdot \alpha^q$ where r, q

are natural numbers and $r < t$. More precisely, for every natural number n, $exp_\epsilon(n) = \epsilon^r \cdot \alpha^q$ where r is the remainder and q is the quotient of n divided by t. Hence exp_ϵ is again definable in $(\mathbf{C},\, \mathbf{Z})$ (as exponentiation with respect to the rational basis α is definable).

The following proposition generalizes all the previous examples.

Proposition 2.3 *If ϵ is algebraic, then exp_ϵ is $\emptyset$-definable in $(\mathbf{C},\, \mathbf{Z})$.*

Proof. Let $p(x)$ be the minimal polynomial of ϵ over the rationals and let d be its degree. Then the elements in K can be uniquely written as $a_0 + a_1\epsilon + \ldots + a_{d-1}\epsilon^{d-1}$ where the a_j $(j < d)$ are rational. Hence K can be identified with $\mathbf{Q}^d$ where addition and multiplication are introduced in the right way (and $\mathbf{Q}$ consists of the d-tuples of rationals whose second, third, ... and last components are 0, while ϵ is $(0,\, 1,\, 0,\, \ldots,\, 0)$). Indeed, by using the representation of rationals as quotients of two coprime integers r, s with $s > 0$ and some effective bijection between $\mathbf{Z}$ and $\mathbf{N}$, we can identify K with a suitable recursive subset of $\mathbf{N}^{2d}$. The function exp_ϵ (adapted to this setting) is explicitly computable, in other words recursive, hence arithmetical. As the addition and multiplication of natural numbers are definable in the ring of integers (and in the field of rationals), it turns out that even in this general framework, exp_ϵ is definable in $(\mathbf{C},\, \mathbf{Z})$. $\dashv$

Let us consider now a transcendental ϵ. Since the resulting structure $(\mathbf{C},\, \mathbf{Z},\, exp_\epsilon)$ has a unique isomorphism type in this setting, we can assume $\epsilon = e$, hence we will let $exp_\epsilon = exp$. Then $E(\mathbf{C},\, \mathbf{Z},\, exp) = \mathbf{Z}[e,\, e^{-1}]$ and $K(\mathbf{C},\, \mathbf{Z},\, exp) = \mathbf{Q}(e)$. But now exp is not $\emptyset$-definable in $(\mathbf{C},\, \mathbf{Z})$; in fact a subset $\emptyset$-definable in this structure and containing some transcendental number must include all the transcendental numbers [5], while $exp(\mathbf{Z})$ contains e but is countable and hence exclude most transcendental numbers. Actually a stronger result holds.

Proposition 2.4 *The exponential function exp is not definable in* $(\mathbf{C},\, \mathbf{Z})$ *(even using parameters).*

Proof. It suffices to prove that $exp(\mathbf{N})$, that is, the set of powers e^n with n a natural number, is not definable in $(\mathbf{C},\, \mathbf{Z})$.
Suppose on the contrary that $exp(\mathbf{N})$ is definable, say by a formula $\varphi(v,\, e,\, \vec{a})$ (let us explicitly include for simplicity e itself among the parameters). We can assume that e, $\vec{a}$ are algebraically independent over $\mathbf{Q}$. In fact, if this is not the case then we can arrange $\vec{a}$ as $(\vec{a'},\, b)$ where b is algebraic over $\mathbf{Q}(e,\, \vec{a'})$. Let $s(x)$ be the minimal polynomial of b over $\mathbf{Q}(e,\, \vec{a'})$, and b' be any other root of $s(x)$. Then there is an automorphism of $(\mathbf{C},\, \mathbf{Z})$ fixing e (and hence $exp(\mathbf{N})$) and $\vec{a'}$ pointwise, sending b to b'. So the formula $\varphi(v,\, e,\, \vec{a'},\, b')$ built by replacing b by b' in $\varphi(v,\, e,\, \vec{a})$ still defines $exp(\mathbf{N})$. Then $exp(\mathbf{N})$ can be defined without involving b, by the formula $\forall x\, (s(x) = 0 \longrightarrow \varphi(v,\, e,\, \vec{a'},\, x))$. On this basis it is straightforward to develop a suitable induction argument leading to the conclusion that $exp(\mathbf{N})$ can be defined as claimed, that is, by a tuple $\vec{a}$ of parameters algebraically independent over $\mathbf{Q}(e)$.
Now we claim that, for every formula $\varphi(v,\, w,\, \vec{u})$ of the language of $(\mathbf{C},\, \mathbf{Z})$, there exists a natural number $N = N(\varphi)$ such that either

(i) for every $\vec{a}$ algebraically independent over $\mathbf{Q}(e)$ the set $\varphi(v, e, \vec{a})$ defines in $(\mathbf{C}, \mathbf{Z})$ is co-countable, or

(ii) for every $\vec{a}$ algebraically independent over $\mathbf{Q}(e)$ the only powers of e it contains are at most $1, e, \ldots, e^N$.

This clearly excludes that $\varphi(v, e, \vec{a})$ defines $exp(\mathbf{N})$.
As the theory of $(\mathbf{C}, \mathbf{Z})$ eliminates quantifiers up to quantification over the predicate for the integers (as shown in [5] in the particular case of $(\mathbf{C}, \mathbf{Z})$ and in [1] in the more general framework of pairs $(\mathcal{M}, P)$ where $\mathcal{M}$ is a strongly minimal structure and P is a unary predicate), we can assume that $\varphi(v, w, \vec{u})$ has the form

$$Q_1 z_1 \in \mathbf{Z} \ldots Q_k z_k \in \mathbf{Z}\, \varphi'(v, w, \vec{u}, \vec{z})$$

where k is a natural number, $\vec{z} = (z_1, \ldots, z_k)$, each Q_j $(1 \leq j \leq k)$ is a quantifier $\forall$ or $\exists$ and $\varphi'(v, w, \vec{u}, \vec{z})$ is a finite disjunction of finite conjunctions of formulas

$$p(v, w, \vec{u}, \vec{z}) = 0, \quad p(v, w, \vec{u}, \vec{z}) \in \mathbf{Z}$$

and negations, where p is any polynomial with coefficients in $\mathbf{Z}$. Thus $p(v, w, \vec{u}, \vec{z})$ can be written as $\sum_{i \leq n} p_i(w, \vec{u}, \vec{z}) v^i$ where the p_i are polynomials with coefficients in $\mathbf{Z}$.
We will proceed by induction on k. At the end our first induction step, we will make more precise our assumptions on N, in particular how it depends on φ.
Suppose $k = 0$, in other words $\varphi(v, w, \vec{u})$ is quantifier free and $\vec{z}$ is empty. As the conclusions of the claim about $\varphi(v, w, \vec{u})$ are preserved under finite disjunctions and conjunctions we can assume that $\varphi(v, w, \vec{u})$ is $p(v, w, \vec{u}) = 0$ or $p(v, w, \vec{u}) \in \mathbf{Z}$ (or negation) where p a polynomial with integer coefficients. Consider the $p_i(w, \vec{u})$ as polynomials in w with coefficients in $\mathbf{Z}[\vec{u}]$.
If some $p_i(w, \vec{u})$ is non zero, then let N be the maximal degree of the $p_i(w, \vec{u})$ with respect to w. Take a tuple $\vec{a}$ algebraically independent over $\mathbf{Q}(e)$. As e is transcendental over $\mathbf{Q}(\vec{a})$, for any $m > N$ e^m does not annihilate $p(v, e, \vec{a})$ or give it an integer value; otherwise, as the coefficients $p_i(w, \vec{a})$ have degree at most N, for $m > N$ $p(v^m, v, \vec{a})$ would become a nonzero polynomial over $\mathbf{Q}(\vec{a})$ annihilated by e, which is clearly impossible. Thus the only powers of e that can satisfy $\varphi(v, e, \vec{a})$ are among $1, e, \ldots, e^N$.
Otherwise, when $p(v, w, \vec{u})$ is identically 0 with respect to w, the set of roots of $p(v, e, \vec{a})$ is all of $\mathbf{C}$, and the same is true of the set of complex numbers giving it an integer value.
Passing to negations yields either cofinite or empty sets. This proves our claim in the case $k = 0$.
Observe that the bound N depends on the degrees of the $p_i(w, \vec{u})$ with respect to w rather than directly on φ. Even if the coefficients of the $p_i(w, \vec{u})$ range over all integers, N remains the same, or possibly decreases when some $p_i(w, \vec{u})$ becomes zero. Actually this is what we assume in the next steps of our induction argument.
Now take $k > 0$. Suppose our claim is holds for $k-1$ and we will prove it is also true for k. We can assume that $\varphi(v, w, \vec{u})$ is of the form $\forall z \in \mathbf{Z}\, \varphi''(v, w, \vec{u}, z)$

or $\exists z \in \mathbf{Z}\, \varphi''(v, w, \vec{u}, z)$ where for every integer n, $\varphi''(v, w, \vec{u}, n)$ satisfies our claim, in other words, either $\varphi''(v, e, \vec{a}, n)$ defines a co-countable set for every $\vec{a}$ algebraically independent over $\mathbf{Q}(e)$ and for every n, or the only powers of e satisfying it are among $1, e, \ldots, e^N$ for every $\vec{a}$ and n.
The intersections and unions of the sets the various $\varphi(v, e, \vec{a}, n)$ define in $(\mathbf{C}, \mathbf{Z})$ when n ranges over integers are co-countable, or exclude any power of e having exponent $> N$ (in particular, recall that a countable intersection of co-countable sets is co-countable).
This completes the proof of the claim and of the whole proposition. $\dashv$

3 An algebraic analysis of $(\mathbf{C}, \mathbf{Z}, exp)$

We continue our study of $(\mathbf{C}, \mathbf{Z}, exp)$ where exp denotes exponentiation with respect to e, emphasizing some algebraic properties of this structure which will be helpful, and in some cases crucial to results in the remainder of this paper. First let us deal with the following Schanuel property, in which we use a large saturated elementary extension $\mathcal{U}$ of $(\mathbf{C}, \mathbf{Z}, exp)$.

Proposition 3.1 *Let $M_0 = 1, M_1, \ldots, M_k \in Z(\mathcal{C})$ be linearly independent over $\mathbf{Q}$ (the standard rationals). Then $exp(M_0), exp(M_1), \ldots, exp(M_k)$ are algebraically independent over $Q(\mathcal{U})$ (the non-standard rationals).*

Proof. By compactness, it is sufficient, and indeed equivalent, to show that for every non-zero polynomial $p(v, w_1, \ldots, w_k, \vec{z})$ with coefficients in $\mathbf{Z}$, there exists a bound $H = H(p)$, only depending on p, such that, for every choice of a tuple $\vec{a}$ in $\mathbf{Q}$ with $p(v, w_1, \ldots, w_k, \vec{a}) \neq 0$ and every $(m_1, \ldots, m_k) \in \mathbf{Z}^k$ satisfying

$$\textstyle\sum_{j \leq k} t_j m_j \neq 0 \text{ for every choice of integers } t_j,\ |t_j| < H,\ t_j \text{ not all zero,}$$

$p(e, exp(m_1), \ldots, exp(m_k), \vec{a}) \neq 0$.
To prove that, let us state in a more general setting, the first step of the induction argument proving Proposition 2.4.

Lemma 3.2 *Let F be any field, b be transcendental over F, $p(v, w_1, \ldots, w_k)$ be a polynomial over F with degree $N_0 > 0$ in v and $N_j > 0$ in w_j for every j with $1 \leq j \leq k$. Choose integers m_j $(j \leq k)$ such that $m_0 = 1$, $m_1 > N_0$, $m_2 > m_1 \cdot N_1 + N_0, \ldots, m_k > m_{k-1} \cdot N_{k-1} + \ldots + m_1 \cdot N_1 + N_0$. Then $p(b^{m_0}, b^{m_1}, \ldots, b^{m_k}) \neq 0$.*

Proof. Under the assumptions on the m_j, $p(v, v^{m_1}, \ldots, v^{m_k})$ is a nonzero polynomial in v over F, and consequently cannot admit b as a root. $\dashv$

Actually a more general result holds.

Lemma 3.3 *Let F be a field, b be transcendental over F, $p(v, w_1, \ldots, w_k)$ be a polynomial over F with degree $N_0 > 0$ in v and $N_j > 0$ in w_j for $1 \leq j \leq k$. Choose integers m_j $(j \leq k)$ such that $1 = m_0 < m_1 < \ldots < m_k$ and the only linear dependence relation $\sum_{j \leq k} t_j m_j$ with integer coefficients t_j $(|t_j| \leq N_j$ for* *every $j \leq k$) among the m_j is the trivial one (when all the t_j's are 0). Then* $p(b^{m_0}, b^{m_1}, \ldots, b^{m_k}) \neq 0$.

Proof. In fact our assumptions are sufficient to ensure that the exponents of the various powers of b in $p(b, b^{m_1}, \ldots, b^{m_k})$ are pairwise different. Thus the transcendence of b over F implies our claim. $\dashv$

Applying this to the case when F is the rational field and $b = e$, we obtain H as the maximum of the N_j. Notice that this bound H does not depend on the coefficients of p, but only on its degrees. This concludes the proof of Proposition 3.1. $\dashv$

Observe that in the particular setting of $\mathbf{Q}$ and e the statements of Lemmas 3.2 and 3.3 can be expressed by infinitely many first order sentences of L, one sentence for every tuple N_j ($j \leq k$) of positive "standard" integers, saying that for every polynomial $p(v, w_1, \ldots, w_k)$ with coefficients in Q, and degree N_0 in v, N_j in w_j ($1 \leq j \leq k$), and for every choice of $m_0, m_1, \ldots, m_k$ as explained in the lemmas, $p(exp(m_0), exp(m_1), \ldots, exp(m_k)) \neq 0$. The same is true of Proposition 3.1 itself, that can be can be expressed in a first order way by infinitely many sentences, one for every polynomial p as in the statement of the proposition with the corresponding bound H. Also, observe that an estimate of H with respect to p is explicitly given.

We will now examine how exp function extends from the integers to the rationals. To introduce this problem from a slightly different perspective, think of a tuple of positive integers M_j ($j \leq k$, $M_0 < M_1 < \ldots < M_k$, possibly $M_0 > 1$) satisfying some equality

$$(\star) \qquad tM_k = \sum_{j<k} t_j M_j$$

where the coefficients t, t_j ($j < k$) are also integers and $t \neq 0$. We can assume $t > 0$, and even minimal with respect to these properties. This implies that the greatest common divisor of $t, t_0, \ldots, t_{k-1}$ is 1. Moreover

$$(e^{M_k})^t = e^{\sum_{j<k} t_j M_j} = \prod_{j<k} (e^{M_j})^{t_j}$$

hence e^{M_k} is a root of the polynomial $x^t - \prod_{j<k}(e^{M_j})^{t_j}$, and indeed the only root in $exp(\mathbf{Z})$. We would like to determine how to single out $exp(M_k)$ among the various t-th roots of $x^t - \prod_{j<k}(e^{M_j})^{t_j}$ over the field

$$\mathbf{Q}(exp(M_0), exp(M_1), \ldots, exp(M_{k-1}))$$

via mere algebraic methods, without reference to exp. The following proposition clarifies this question.

Proposition 3.4 *For $M_0 < M_1 < \ldots < M_{k-1}$ positive integers, $t, t_1, \ldots, t_{k-1}$ integers, $t > 0$, $t, t_1, \ldots, t_{k-1}$ coprime, $x^t - \prod_{j<k}(e^{M_j})^{t_j}$ is irreducible over* $\mathbf{Q}(e^{M_0}, e^{M_1}, \ldots, e^{M_{k-1}})$.

Proof. First observe, that if M denotes the greatest common divisor of the M_j $(j < k)$, then

$$\mathbf{Q}(e^{M_0}, \ldots, e^{M_{k-1}}) = \mathbf{Q}(e^M).$$

Also notice that condition $(\star)$ can be written as

$$(\star)' \quad tM_k = qM$$

for some suitable integer q; moreover t is minimal with respect to this property, which implies that t and q are coprime, and consequently that t divides M. We are led in this way to consider $x^t - e^{qM}$ as a polynomial over $\mathbf{Q}(e^{qM})$. So Proposition 3.4 becomes a consequence of the following lemma.

Lemma 3.5 *If $t > 0$, $M > 0$ and q are integers, t and q are coprime and t divides M, then $x^t - e^{qM}$ is irreducible in $\mathbf{Q}(e^{qM})[x]$.*

Proof. Let ζ_t denote a primitive t-th root of 1 in $\mathbf{C}$. Thus $x^t - e^{qM}$ decomposes in $\mathbf{C}[x]$ as

$$x^t - e^{qM} = \prod_{r \leq t} (x - \zeta_t^r e^{\frac{qrM}{t}}).$$

Suppose for a contradiction that $x^t - e^{qM}$ is not irreducible over $\mathbf{Q}(e^{qM})$. Each irreducible factor in its decompositions has coefficients of the form $h(e^{\frac{qrM}{t}})$ where $h(x)$ is a polynomial in $\mathbf{Q}[x]$ possibly 0, or of degree $< t$. On the other hand the same coefficient can be written as $f(e^{qM}) \cdot g(e^{qM})^{-1}$ where $f(x)$, $g(x) \in \mathbf{Q}[x]$ and $g(x) \neq 0$. Therefore $f(e^{qM}) \cdot h(e^{\frac{qrM}{t}}) = g(e^{qM})$ whence, by the transcendence of e, $h(x)$ has to be constant, possibly 0. This means that the factorization of $x^t - e^{qM}$ over $\mathbf{Q}(e^{qM})$ only involves polynomials with rational coefficients, which is clearly impossible. $\dashv$

Note that the statement of Proposition 3.4 can be expressed in L by infinitely many first order sentences. In fact, take any polynomial $p(x, w_0, \ldots, w_{k-1})$ with coefficients in Z and degree $d < t$ in x; then the coefficients of p with respect to x can be written as sums of monomials $z w_0^{d_0} \ldots w_{k-1}^{d_{k-1}}$ with $z \in Z$ and $d_0, \ldots, d_{k-1}$ natural numbers. Then the first order translation of Proposition 3.4 requires one sentence for every choice of t and t_j, and various d_j $(j < k)$ in two given polynomials p and p' as before; this sentence says, that for every p, p' (meaning for every choice of the various z) and for every $0 < M_0 < M_1 < \ldots < M_{k-1}$ in Z, the product of $p(x, e^{M_0}, \ldots, e^{M_{k-1}})$ and $p'(x, e^{M_0}, \ldots, e^{M_{k-1}})$ cannot equal $x^t - \prod_{j<k} (e^{M_j})^{t_j}$.

4 The transcendental case. An axiomatization

We now propose a tentative axiomatization of the first order theory of $(\mathbf{C}, \mathbf{Z}, exp_\epsilon)$ when ϵ is transcendental. As above, we refer for simplicity to $\epsilon = e$, so to $exp = exp_e$ as the function taking every integer z to e^z. Our axioms are based on the properties of e and exp we emphasized in the previous section, and on

some further features that are mostly trivialities in the framework of ($\mathbf{C}$, $\mathbf{Z}$, exp) but play a more significant role in the other models.
We will deal with L-structures $\mathcal{C}$. Our axioms express in a first order way in L the following.

1. C is an algebraically closed field of characteristic 0 (with respect to $+$, $\cdot$, $-$, 0 and 1).

2. $Z(\mathcal{C})$ is a subring of C with 1 and, as such, is a model of the first order theory of ($\mathbf{Z}$, $+$, $\cdot$, 0, 1), hence, among other properties: is an integral domain with identity 1, and is an ordered domain (by Lagrange's Theorem); however this is the "dark side" of our axiomatization, as the Gödel phenomena forbid a full comprehension of the theory of the ring of integers.

3. $EXP(\mathcal{C})$ (EXP for short) is a 1-1 function of $Z(\mathcal{C})$ to C with the following properties.

   (3.1) EXP is a group morphism of the additive group of $Z(\mathcal{C})$ to the multiplicative group of C (equivalently, $EXP(x+y) = EXP(x) \cdot EXP(y)$ for all $x, y \in Z(\mathcal{C})$ and $EXP(0) = 1$).

   (3.2) $EXP(Z(\mathcal{C}))$ is linearly independent over $Q(\mathcal{C})$.

   (3.3) (*A Schanuel condition*) For every positive integer k, if $1 = M_0, M_1, \ldots, M_k \in Z(\mathcal{C})$ are linearly independent over $\mathbf{Q}$, then $EXP(M_0)$, $EXP(M_1), \ldots, EXP(M_k)$ are algebraically independent over $Q(\mathcal{C})$.

   (3.4) (*Extracting t-th roots*) For every choice of k, t, t_j ($j < k$) in $\mathbf{Z}$ with $k > 0$, $t > 0$ and $t, t_0, \ldots, t_{k-1}$ coprime, for every $0 < M_0 < \ldots < M_{k-1}$ in $Z(\mathcal{C})$ the polynomial $x^t - \prod_{j<k} EXP(M_j)^{t_j}$ is irreducible over $Q(\mathcal{C})(EXP(M_0), EXP(M_1), \ldots, EXP(M_{k-1}))$.

   (3.5) For every positive integer n, the polynomial $x^n - 2$ is irreducible over $Q(\mathcal{C})$.

   (3.6) (*A closure condition*) For every polynomial $q(\vec{x}, \vec{y}) \in \mathbf{Q}[\vec{x}, \vec{y}]$ and $\vec{a} \in \mathbf{Q}(EXP(1))^{alg}$, if no $\vec{b} \in \mathbf{Z}[EXP(1), EXP(-1)]$ satisfies $q(\vec{x}, \vec{b}) \neq 0$ and $q(\vec{b}, \vec{a}) = 0$, then no tuple in $E(\mathcal{C})$ has this property.

Let T be the first order theory axiomatized in this way. We will now comment on the various conditions in 3, in particular why they are true in ($\mathbf{C}$, $\mathbf{Z}$, exp) and can be expressed in a first order way in L (possibly by infinitely many sentences). This is clearly true of (3.1).

Remarks 4.1 (3.2) holds in ($\mathbf{C}$, $\mathbf{Z}$, exp) because e is transcendental. Indeed (3.2) implies that in every model $\mathcal{C}$ of T $EXP(1)$ is transcendental over $Q(\mathcal{C})$. Also, it can be expressed by infinitely many first order L-sentences, one for every positive integer k, saying that for every choice of z_j, M_j in $Z(\mathcal{C})$ ($j \leq k$) with $M_0 < M_1 < \ldots < M_k$, if $\sum_{j \leq k} z_j \, EXP(M_j) = 0$, then $z_j = 0$ for every $j \leq k$.

(3.3) corresponds to Proposition 3.1. This was explained in the previous section, including how to write it in a first order way (see the discussion preceding the second proof of Proposition 3.1, and then Lemmas 3.2 and 3.3). Actually a (slightly stronger) first order condition referring to Lemma 3.3 and ensuring (3.3) is the following: For every polynomial $p(x, w_1, \ldots, w_k)$ over $Q(\mathcal{C})$ of degree $N_0 > 0$ in x and $N_j > 0$ in w_j $(1 \leq j \leq k)$, for every $M_j \in Z(\mathcal{C})$ $(j \leq k)$ such that $1 = M_0 < M_1 < \ldots < M_k$ and the only linear dependence relation $\sum_{j \leq k} z_j M_j$ with integer coefficients z_j $(j \leq k$, $|z_j| \leq N_j)$ –caution: the z_j are "standard"!– among the M_j is the trivial one (when all the z_j are 0),

$$p(EXP(1), EXP(M_1), \ldots, EXP(M_k)) \neq 0.$$

(3.4) was treated in the previous section. Specifically Proposition 3.4 shows that it holds in (**C**, **Z**, *exp*), while the last lines of § 3 explain how to write it in a first order way in L.

(3.5) is a well known fact valid in (**C**, **Z**, *exp*), and can be easily expressed in L in a first order way.

(3.6) is clearly true in (**C**, **Z**, *exp*), where E is interpreted as $\mathbf{Z}[e, e^{-1}]$. Moreover it can be suitably expressed in a first order way in L by infinitely many sentences, one for every polynomial q and for every type of a tuple $\vec{a}$ over $\mathbf{Q}(e)$ (in the language of fields) containing $q(\vec{v}, \vec{b}) \neq 0$ for all $\vec{b}$ in $\mathbf{Z}[e, e^{-1}]$; this sentence says that no tuple $\vec{b}$ in $Z(\mathcal{C})$ satisfies both $q(\vec{x}, \vec{b}) \neq 0$ and $q(\vec{a}, \vec{b}) = 0$. Quantifying over types of tuples $\vec{a} = (a_1, \ldots, a_n)$ in $\mathbf{Q}(e)^{alg}$ over $\mathbf{Q}(e)$ can be stated as *"for every v_1 satisfying the minimal polynomial of a_1 over $\mathbf{Q}(e)$, for every v_2 satisfying the minimal polynomial of a_2 over $\mathbf{Q}(e, v_1)$ and so on"*. In fact these conditions on minimal polynomials determine the type of $\vec{a}$ over $\mathbf{Q}(e)$ and it is easily seen, that if $\vec{a'}$ is another tuple satisfying them, then there is field automorphism of **C** fixing $\mathbf{Q}(e)$ pointwise and sending $\vec{a}$ to $\vec{a'}$, hence for every $\vec{b} \in \mathbf{Z}[EXP(1), EXP(-1)]$ with $q(\vec{x}, \vec{b}) \neq 0$, $q(\vec{a}, \vec{b}) = 0$ holds if and only if $q(\vec{a'}, \vec{b}) = 0$ does.
Regrettably, we do not see how to explicitly decide and list the pairs consisting of a polynomial and a type and occurring in these sentences.

We will refer to (**C**, **Z**, *exp*) as the *standard model* of T. We will now state some simple consequences of the axioms of T.

Remarks 4.2 Here $\mathcal{C}$ denotes an arbitrary model $(C, Z(\mathcal{C}), EXP)$ of T.

1. $Z(\mathcal{C}) \cap EXP(Z(\mathcal{C})) = \{1\}$.

2. For every positive (standard) integer t and for every a and b in $Z(\mathcal{C})$, if $EXP(a)^t = EXP(b)^t$, then $a = b$ (as $EXP(a)^t = EXP(t \cdot a)$ and similarly for b, moreover EXP is injective).

3. Let F be any subfield of C containing $E(\mathcal{C})$ (equivalently, $K(\mathcal{C})$). If a and b are two elements of C transcendental over F, then there is an automorphism f of $\mathcal{C}$ as a field fixing F pointwise and taking a to b. As f acts identically on F, f is also an automorphism of L. In particular a and b have the same type over F (with respect to L). Also, if X is an F-definable set, then X either includes or excludes all the elements of C transcendental over F.

Corollary 4.3 *The standard model of T $(\mathbf{C}, \mathbf{Z}, exp)$ is quasi minimal.*

Proof. Let X be a definable subset of the complex field and let $\vec{a}$ be a tuple of parameters defining X. Then X either excludes or includes all the elements transcendental over $\mathbf{Q}(e, \vec{a})$. Accordingly X is countable or co-countable. $\dashv$

Corollary 4.4 *The model theoretic algebraic closure of $\emptyset$ $acl(\emptyset)$ in T equals the field theoretic algebraic closure $\mathbf{Q}(EXP(1))^{alg}$ of $\mathbf{Q}(EXP(1))$.*

Proof. It is clear that $\supseteq$ holds. On the other hand no finite $\emptyset$-definable set in the standard model can include an element transcendental over $\mathbf{Q}(e)$ (otherwise it contains infinitely many transcendental elements). $\dashv$

Lemma 4.5 *Let $\mathcal{C}$ be any model of T. Then every element of $E(\mathcal{C})$ decomposes uniquely as $z_0 + \sum_{1 \leq j \leq k} z_j\, EXP(M_j)$ where k is a natural number, the z_j and the M_j are in $Z(\mathcal{C})$ and $M_1 < \ldots < M_k$.*

Proof. Every element of $E(\mathcal{C})$ can be obtained by adding and multiplying integers and values of EXP. Integers are closed under both addition and multiplication, and values of EXP under multiplication. Also, the distributivity law can be applied. This ultimately yields a decomposition as claimed. Axiom (3.2) ensures that this decomposition is unique. $\dashv$

Corollary 4.6 *$E(\mathcal{C})$ and $K(\mathcal{C})$ are not definable in $\mathcal{C}$.*

Proof. In fact $E(\mathcal{C})$ includes elements $z_0 + \sum_{1 \leq j \leq k} z_j\, EXP(M_j)$ with an arbitrarily large k. So a standard compactness argument applies and proves our claim. $\dashv$

Proposition 4.7 *Let $\mathcal{C} = (C, Z(\mathcal{C}), EXP)$ be a model of T, F be an algebraically closed proper subfield of C extending $K(\mathcal{C})$. Then $(F, Z(\mathcal{C}), EXP)$ is an elementary substructure of $\mathcal{C}$, and in particular is a model of T. Also, F is not definable in $\mathcal{C}$.*

Proof. We apply the Tarski-Vaught criterion and show that F is the domain of an elementary substructure $\mathcal{F}$ of $\mathcal{C}$ (observe that, as $Z(\mathcal{C})$ is a subring of F and $EXP \subseteq F^2$, in this substructure $Z(\mathcal{F}) = Z(\mathcal{C})$ and EXP is the restriction of the exponential function from $\mathcal{C}$ to F^2). Take any formula $\varphi(v, \vec{a})$ with parameters $\vec{a}$ from F. We will show that if $\mathcal{C} \models \exists v\, \varphi(v, \vec{a})$, then there is some $b \in F$ such that $\mathcal{C} \models \varphi(b, \vec{a})$.
Suppose this is false. There is at least one element satisfying $\varphi(v, \vec{a})$ in $\mathcal{C}$, and

this element has to be transcendental over F. By Remark 3 in 4.2, $C - F \subseteq \varphi(\mathcal{C}, \vec{a})$. But no element of F can belong to $\varphi(\mathcal{C}, \vec{a})$, so $C - F = \varphi(\mathcal{C}, \vec{a})$, equivalently $F = \neg\varphi(\mathcal{C}, \vec{a})$. So it is sufficient to prove that F cannot be defined in $\mathcal{C}$ in a first order way. Note that this is an interesting fact in its own right (and in fact we state it separately in our proposition). We will refer to a large saturated elementary extension $\mathcal{U}$ of $\mathcal{C}$.
Let us first assume $F = \mathbf{Q}(e)^{alg}$ and $K(\mathcal{C}) = \mathbf{Q}(e)$. Observe that every element of $\mathcal{C}$ satisfying $\varphi(v, \vec{a})$ is transcendental over $K(\mathcal{C})$ because F extends $K(\mathcal{C})$. Consequently the same is true in $\mathcal{U}$ with respect to $K(\mathcal{U})$. Take $c \in C$ transcendental over $\mathbf{Q}(e)$, then $\varphi(c, \vec{a})$ holds in $\mathcal{C}$ and in $\mathcal{U}$, hence c is transcendental over $K(\mathcal{U})$. Now consider the 1-type Γ over $\mathbf{Q}(e)$ consisting of:

- $\neg\varphi(v, \vec{a})$,
- the formulas saying that v does not annihilate any polynomial of degree n with coefficients from K (equivalently from E) when n ranges over the positive integers (there is a formula for every n and for every choice of coefficients in E according to the representation described in Lemma 4.5).

This type is finitely satisfiable in $\mathcal{C}$. In fact take a finite subset Γ_0 of Γ, say consisting of $\neg\varphi(v, \vec{a})$ and certain formulas of the second kind corresponding to degrees smaller than a given N. For $n \geq N$ the polynomial $x^n - 2$ is irreducible over $\mathbf{Q}(e)$, hence an n-th root of 2 satisfies Γ_0.
By compactness there is some element $c' \in U$ satisfying Γ. Both c and c' are transcendental over $K(\mathcal{U})$. Then there is an automorphism of $\mathcal{U}$ –as a field, and as a structure of L– fixing $K(\mathcal{U})$, and in particular $\mathbf{Q}(e)$, pointwise and sending c to c'. But c satisfies $\varphi(v, \vec{a})$ and c' does not – a contradiction.
Now take any F with $Z(\mathcal{F}) = Z(\mathcal{C})$. We can proceed as for $\mathbf{Q}(e)^{alg}$. The crucial point is again to satisfy any finite $\Gamma_0 \supseteq \Gamma$ inside $\mathcal{C}$. The polynomials in Γ_0 have again degree smaller than some fixed N, but their coefficients may involve, in addition to arbitrary elements from $K(\mathcal{C})$ some further parameters $\vec{s}$ from $F - K(\mathcal{C})$. Again, it suffices to find some element in F that is algebraic of degree at least N over $K(\mathcal{C})(\vec{s})$.
It is easily seen that one can assume that $\vec{s}$ is algebraically independent over $K(\mathcal{C})$. In fact, if this is the case and $\vec{t}$ is a tuple of elements algebraic over $K(\mathcal{C})(\vec{s})$ such that the degree of $K(\mathcal{C})(\vec{s}, \vec{t})$ over $K(\mathcal{C})(\vec{s})$ is d, it suffices to take an element $b \in F$ algebraic of degree at least $N \times d$ over $K(\mathcal{C})(\vec{s})$ to guarantee that the degree of $K(\mathcal{C})(\vec{s}, \vec{t}, b)$ over $K(\mathcal{C})(\vec{s}, \vec{t})$ is at least N.
Hence we can assume that $\vec{s}$ is algebraically independent over $K(\mathcal{C})$. If the transcendence degree of F over $K(\mathcal{C})$ is greater than the length of $\vec{s}$ then we are done. If this is not the case, we can suppose that $F = K(\mathcal{C})(\vec{s})^{alg}$. By (3.4), for $n \geq N$ $x^n - 2$ is irreducible over $K(\mathcal{C})$ and consequently over $K(\mathcal{C})(\vec{s})$.
In conclusion F cannot be defined by a first order formula in $\mathcal{C}$. Therefore F is the domain of an elementary substructure of $\mathcal{C}$ as claimed. $\dashv$

Observe that the previous proof uses only some very basic properties of EXP, and does not require all the axioms of T.

By Proposition 4.7, $\mathcal{C}_0 = (\mathbf{Q}(e)^{alg}, \mathbf{Z}, exp)$ is an elementary substructure of the standard model $(\mathbf{C}, \mathbf{Z}, exp)$ and so is a model of T. Actually $\mathcal{C}_0$, as a countable atomic model of the first order complete theory of $(\mathbf{C}, \mathbf{Z}, exp)$, is a prime model of this theory. Also, the following fact is easy to check.

Remark 4.8 $\mathcal{C}_0$ is embeddable in every model $\mathcal{C} = (C, Z, EXP)$ of T.
In fact, as C has characteristic 0 and $EXP(1)$ is transcendental over $Q(\mathcal{C})$, $\mathbf{Q}(EXP(1))^{alg}$ –and, through it, $\mathbf{Q}(e)^{alg}$ itself– is embeddable in C as a subfield.
It is clear that the intersection of this subfield and $Z(\mathcal{C})$ is just an isomorphic copy of the ring of integers, but nothing more. In fact, by (3.2) –more precisely, by the transcendence of $EXP(1)$ over $Z(\mathcal{C})$– any nonstandard integer $z > 0$ algebraic over $\mathbf{Q}(EXP(1))$ should be algebraic over $\mathbf{Q}$, which is clearly a contradiction.
Finally, by (3.1), EXP acts in $Z(\mathcal{C})$ on this copy of $\mathbf{Z}$ just like exponentiation with respect to the basis $EXP(1)$.
In the following we will call this embedding of $\mathcal{C}_0$ into $\mathcal{C}$ –fixing any standard integer pointwise and sending e to $EXP(1)$– *canonical*.

Unfortunately, we cannot deduce that $\mathcal{C}_0$ is a prime model of T, because we do not know whether T is complete. Indeed the fact that $\mathcal{C}_0$ is a prime model is just equivalent to the completeness of T. So the basic question to be answered is the following one:

Question. Is $\mathcal{C}_0$ *elementarily* embeddable in any model $\mathcal{C}$ of T? In other words, is $\mathcal{C}_0$ a prime model of T?

Observe that a positive answer to this question cannot be obtained on the basis of Proposition 4.7 because the assumption that $\mathbf{Q}(EXP(1))^{alg}$ extends $K(\mathcal{C})$ may fail. Actually any elementary embedding $\mathcal{C}' \prec \mathcal{C}$ between models of T has to satisfy further conditions, such as the ones we are going to list. For simplicity we assume here that the elementary embedding of $\mathcal{C}'$ into $\mathcal{C}$ is just an inclusion.

(i) $EXP(Z(\mathcal{C}')) = C' \cap EXP(Z(\mathcal{C}))$.
Actually the inclusion $\subseteq$ is trivial. On the other hand, for $b \in C' \cap EXP(Z(\mathcal{C}))$, the sentence $\exists w(EXP(w) = b)$ is true in $\mathcal{C}$, and hence has to be true in $\mathcal{C}'$.

(ii) $E(\mathcal{C}') = C' \cap E(\mathcal{C})$.

(iii) $K(\mathcal{C}') = C' \cap K(\mathcal{C})$.

(iv) $K(\mathcal{C}')^{alg} = C' \cap K(\mathcal{C})^{alg}$.

(v) For every tuple $\vec{a}$ in C' and polynomial $q(\vec{x}, \vec{y}) \in \mathbf{Q}[\vec{x}, \vec{y}]$, if there is some $\vec{b} \in E(\mathcal{C})$ such that $q(\vec{x}, \vec{b}) \neq 0$ but $q(\vec{a}, \vec{b}) = 0$, then there is some tuple in $E(\mathcal{C}')$ with this property.

(vi) For every tuple $\vec{a}$ in C' and polynomial $q(\vec{x}, \vec{y}) \in \mathbf{Q}[\vec{x}, \vec{y}]$, if there is some $\vec{b} \in K(\mathcal{C})$ such that $q(\vec{x}, \vec{b}) \neq 0$ but $q(\vec{a}, \vec{b}) = 0$, then there is some tuple in $K(\mathcal{C}')$ with this property.

It is not difficult to check these conditions one by one. In fact (v) and (vi) are immediate, while (ii), (iii), (iv) can be handled as (i). However it is enough to show (v) –in addition to (i)– because (v) implies the remaining ones. Let us explain why.

Remark 4.9 It is clear that (vi) implies (iv) when $\vec{a}$ consists of a single element, and (iv) also implies (iii), when q is $x-y$. Similarly (ii) is a consequence of (v). So it remains to show that (v) implies (vi).
Fix $\vec{a} \in C'$ and $q(\vec{x}, \vec{y}) \in \mathbf{Q}[\vec{x}, \vec{y}]$ such that some $\vec{b}$ in $K(\mathcal{C})$ satisfies both $q(\vec{x}, \vec{b}) \neq 0$ and $q(\vec{a}, \vec{b}) = 0$. Write each element b of $\vec{b}$ as a quotient $b' \cdot b''^{-1}$ with $b', b'' \in E(\mathcal{C})$ and $b'' \neq 0$. Multiply $q(\vec{x}, \vec{b})$ by the product of the maximal powers of each b'' occurring in the coefficients of $q(\vec{x}, \vec{b})$ and then again by the b'''s (so ultimately by a product of powers $(b'')^{d_b}$ for some suitable positive integer d_b), and create in this way a polynomial in $E(\mathcal{C})$. Then replace all the b''s and the b'''s by new corresponding variables y' and y''. One gets a polynomial $q'(\vec{x}, \vec{y'}, \vec{y''})$ with rational coefficients such that

$$q'(\vec{x}, \vec{b'}, \vec{b''}) \neq 0, \quad q'(\vec{a}, \vec{b'}, \vec{b''}) = 0.$$

By (v) there are tuples $\vec{c'}$, $\vec{c''}$ in $E(\mathcal{C}')$ for which

$$q'(\vec{x}, \vec{c'}, \vec{c''}) \neq 0, \quad q'(\vec{a}, \vec{c'}, \vec{c''}) = 0.$$

In particular every c'' is not zero. At this point divide by the product of the $(c'')^{d_b}$. Let c denote the quotient of a given element c' of $\vec{c'}$ by the corresponding element c'' in $\vec{c''}$. Then each single c is in $K(\mathcal{C})$ and their sequence $\vec{c}$ satisfies

$$q(\vec{x}, \vec{b}) \neq 0, \quad q(\vec{a}, \vec{b}) = 0.$$

This proves (vi).

Lemma 4.10 *For every model $\mathcal{C}$ of T, the canonical embedding of $\mathcal{C}_0$ into $\mathcal{C}$ satisfies (i) and (v) (and hence (ii), (iii), (iv), (vi)).*

Proof. For simplicity we assume that the canonical embedding is just an inclusion, so $e = EXP(1)$ in $\mathcal{C}$. Then (i) follows from (3.3), in fact, for z a non standard integer, $EXP(z)$ and $EXP(1)$ have to be algebraically independent over $Q(\mathcal{C})$ and consequently over $\mathbf{Q}$. Furthermore (v) directly follows from (3.6), because $K(\mathcal{C}_0)^{alg} = C_0$ and $E(\mathcal{C}_0) = \mathbf{Z}[e, e^{-1}]$. $\dashv$

Before concluding this section, let us emphasize two notable consequence of (v), using the same notation as in (v).

Lemma 4.11 *Assume (v) holds. Then a tuple $\vec{a} \in C'$ algebraically independent over $K(\mathcal{C}')$ is also algebraically independent over $K(\mathcal{C})$.*

Proof. Actually this is a consequence of (vi). $\dashv$

Lemma 4.12 *Assume (v) (actually (vi)). Let $\vec{a} \in C'$, $s \in K(\mathcal{C}')^{alg}$. Then s has the same minimal polynomial over $K(\mathcal{C}')(\vec{a})$ and over $K(\mathcal{C})(\vec{a})$.*

Proof. Otherwise the latter minimal polynomial $q(x, \vec{a}, \vec{b})$ (with $\vec{b} \in K(\mathcal{C})$) divides the former but has a smaller degree. Also, we can assume $q(x, \vec{a}, \vec{b})$ is monic, hence $q(x, \vec{x}, \vec{y})$ is monic with respect to x. By (vi) some $\vec{c} \in K(\mathcal{C}')$ satisfies $q(s, \vec{a}, \vec{c}) = 0$ and $q(x, \vec{a}, \vec{c}) \neq 0$. But the degree of $q(x, \vec{a}, \vec{c})$ is smaller than that of the minimal polynomial of s over $K(\mathcal{C}')(\vec{a})$, and this is a contradiction. $\dashv$

5 The transcendental case. Main results

In this section we show that T is complete, and so equals the first order theory of $(\mathbf{C}, \mathbf{Z}, exp)$. An investigation of 1-types over the empty set in an arbitrary model $\mathcal{C}$ of T will be useful in our proof. Over certain models this classification of types is very simple. For instance, in the standard model $K(\mathcal{C}) = \mathbf{Q}(e)$, $\mathbf{Q}(e)^{alg}$ equals $acl(\emptyset)$ and then only one non algebraic 1-type is realized, that of elements transcendental over $K(\mathcal{C})$.
Things change when we look at arbitrary models of T. To obtain a complete picture of this general case, we refer to a big saturated model $\mathcal{C}$ of T.
Again there is a unique 1-type for all the elements transcendental over $K(\mathcal{C})$.
Moreover the elements lying out of $K(\mathcal{C})$ but algebraic over it can be treated in terms of their minimal polynomials and hence of the ordered sequences of the corresponding coefficients in $K(\mathcal{C})$.
On the other hand the elements of $K(\mathcal{C})$ can be viewed as fractions of elements in $E(\mathcal{C})$.
So it is sufficient to deal with a generic element b of $E(\mathcal{C})$. By Lemma 4.5 b decomposes uniquely as $z_0 + \sum_{1 \leq j \leq k} z_j\, EXP(M_j)$ with k a natural number, z_j, $M_j \in Z(\mathcal{C})$ for every j and $M_1 < \ldots < M_k$. Put for simplicity $\vec{z} = (z_0, z_1, \ldots, z_k)$ and $\vec{M} = (M_1, \ldots, M_k)$. The question here is whether the type of the tuple $(\vec{z}, \vec{M})$ over $\emptyset$ in the theory of the ring $\mathbf{Z}$ determines that of b in T, or the latter requires additional information.
For simplicity let us rearrange $(\vec{z}, \vec{M})$ as a single tuple and (by slightly changing our notation) let us represent it as $\vec{M} = (M_0, M_1, \ldots, M_k)$ where $M_0 = 1$. Without loss of generality for our purposes we can assume that all the M_j are positive (if not, we replace any negative M_j by $-M_j$ and $EXP(M_j)$ by its inverse), and indeed that $M_0 < M_1 < \ldots < M_k$. As every positive integer N satisfies $EXP(N) = EXP(1)^N$, we can also assume that all the M_j with $j > 0$ are not "standard". Keeping this notation we prove:

Lemma 5.1 *The type of $\vec{M}$ over $\emptyset$ in the theory of the ring of integers fully determines the type of $\vec{M}$ (and $EXP(\vec{M})$) over $\emptyset$ in T.*

As said, the Schanuel Property (3.3) plays a key role here, as well as (3.4).

Proof. Let us examine the elements of the tuple $\vec{M}$ one by one, by induction on the index $j \leq k$.

First suppose $j = 0, 1$. By (3.2) $EXP(M_0)$ is transcendental over $Q(\mathcal{C})$, and indeed $EXP(M_0)$ and $EXP(M_1)$ are algebraically independent over $Q(\mathcal{C})$. The set of first order statements of these properties determines the type of $\vec{M}$ over the empty set in T.

Now take j with $1 \leq j \leq k$ and look at M_{j+1}. Up to rearranging the indexes i with $1 \leq i \leq j$, we can assume that, for some suitable $h \leq j$, $EXP(M_0)$ and the $EXP(M_i)$ with $1 \leq i \leq h$ are algebraically independent over $Q(\mathcal{C})$, while the remaining $EXP(M_i)$ ($h < i \leq j$) are algebraic over the extension of $Q(\mathcal{C})$ by the previous ones. This can be obtained without changing the order of the various M_i (if necessary, replace any M_i with $i > h$ by $M_i + M_h$). By (3.3) no linear dependence relation $\sum_{i \leq h} t_i M_i = 0$ with integer coefficients t_i can link the M_i (with the only exception of the trivial one, that whose coefficients are 0).

Case 1: $M_0, \ldots, M_h, M_{j+1}$ are linearly independent over the rationals.

Thus by (3.3) $EXP(M_{j+1})$ is algebraically independent from the $EXP(M_i)$ (with $i \leq h$ and consequently with $i \leq j$) over $Q(\mathcal{C})$, which determines its type.

Case 2: $M_0, \ldots, M_h, M_{j+1}$ are linearly dependent over the rationals.

Then there is some nontrivial linear dependence relation $tM_{j+1} + \sum_{i \leq h} t_i M_i = 0$ with "standard" integer coefficients. Due to the assumptions on the M_i with $i \leq h$, it must be the case that $t \neq 0$. Of course we can assume t is positive. Also, we can extend our investigation to all equalities of this form, possibly involving even the M_i with $h < i \leq j$. Choose t minimal, so a generator of the ideal of $\mathbf{Z}$ consisting of the integers accompanying M_{j+1} in one of these equalities. Choose the corresponding t_i ($i \leq j$). Observe that by the minimality of t, the greatest common divisor of t and the t_i is 1. Of course the type of $\vec{M}$ (in the theory of integers) contains the formula saying that t divides $\sum_{i \leq j} t_i M_i$ and identifies M_{j+1} as the corresponding quotient.

Observe $EXP(M_{j+1})^t = \prod_{i \leq j} EXP(M_i)^{t_i}$; in other words $EXP(M_{j+1})$ is a root of the polynomial $x^t - \prod_{i \leq j} EXP(M_i)^{t_i}$. By (3.4), this polynomial is irreducible over

$$Q(\mathcal{C})(EXP(M_0), EXP(M_1), \ldots, EXP(M_j))$$

and consequently over $\mathbf{Q}(\vec{M}, EXP(M_0), EXP(M_1), \ldots, EXP(M_j))$, which identifies $EXP(M_{j+1})$ without any ambiguity and determines the type of $\vec{M}$.

Let $\vec{M}'$ be a tuple in $Z(\mathcal{C})$ admitting the same type as $\vec{M}$ in the theory of the ring of integers. Then there is an automorphism of $Z(\mathcal{C})$ (in the language of rings) sending $\vec{M}$ to $\vec{M}'$, and this automorphism can be extended to an automorphism of the whole L-structure $\mathcal{C}$ sending $EXP(\vec{M})$ to $EXP(\vec{M}')$. $\dashv$

Proposition 5.2 *Let $\mathcal{C} = (C, Z(\mathcal{C}), EXP)$ be a model of T and let F be an algebraically closed proper subfield of C. Assume that $F \cap Z(\mathcal{C})$ is an elementary substructure of $Z(\mathcal{C})$ (in the language of rings). Also, assume that:*

(i) $EXP(F) = F \cap EXP(Z(\mathcal{C}))$ *–then we can form the L-structure* $\mathcal{F} = (F, F \cap Z(\mathcal{C}), F^2 \cap EXP)$ *with* $Z(\mathcal{F}) = F \cap Z(\mathcal{C})$*);*

(v) for every $\vec{a}$ *in* F *and polynomial* $q(\vec{x}, \vec{y}) \in \mathbf{Q}[\vec{x}, \vec{y}]$*, if there is some* $\vec{b} \in E(\mathcal{C})$ *such that* $q(\vec{x}, \vec{b}) \neq 0$ *and* $q(\vec{a}, \vec{b}) = 0$*, then there is some tuple in* $E(\mathcal{F})$ *with this property.*

Then $\mathcal{F}$ *is an elementary substructure of* $\mathcal{C}$*.*

Proof. As in Proposition 4.7 we apply the Tarski-Vaught criterion and show that F is the domain of an elementary substructure of $\mathcal{C}$ (of course, this substructure is just $\mathcal{F}$). Accordingly let $\varphi(v, \vec{a})$ be a formula of L with parameters $\vec{a}$ from F such that $\mathcal{C} \models \exists v\, \varphi(v, \vec{a})$. We are looking for some $b \in F$ such that $\mathcal{C} \models \varphi(b, \vec{a})$.

Claim 1: We can assume $\vec{a} = (\vec{a'}, \vec{a''})$ where $\vec{a'}$ is in $Z(\mathcal{F})$ and $\vec{a''}$ is algebraically independent over $K(\mathcal{F})$ (equivalently over $K(\mathcal{C})$).
In fact, observe that for every element a in $\vec{a}$, if $a \in E(\mathcal{C})$ (equivalently, $a \in E(\mathcal{F})$), then a decomposes uniquely as $z_0 + \sum_{1 \leq j \leq h} z_j EXP(M_j)$ with z_j and M_j in $Z(\mathcal{F})$ and $M_1 < \ldots < M_k$, and we can replace a as a parameter using the z_j and M_j; similarly, if $a \in K(\mathcal{C})$ (equivalently $a \in K(\mathcal{F})$), then a can be expressed as a quotient of two elements in $E(\mathcal{F})$ and can be replaced as a parameter by the ordered pair of these elements.
Now decompose $\vec{a}$ as $(\vec{a'}, \vec{a''})$ where $\vec{a''}$ is algebraically independent over $K(\mathcal{F})$ and the elements in $\vec{a'}$ are algebraic over $K(\mathcal{F})(\vec{a})$. Observe that $\vec{a''}$ is algebraically independent also over $K(\mathcal{C})$ (by (v) and Lemma 4.11). Let

- $p_0(w_0, \vec{a''})$ be the minimal polynomial of a'_0 over $K(\mathcal{F})(\vec{a''})$ (and over $K(\mathcal{C})(a''))$, see Lemma 4.12), and
- for every $i < m$ let $p_{i+1}(a'_0, \ldots, a'_i, w_{i+1}, \vec{a''})$ be the minimal polynomial of a'_{i+1} over $K(\mathcal{F})(a'_0, \ldots, a'_i, \vec{a''})$ (and over $K(\mathcal{C})(a'_0, \ldots, a'_i, \vec{a''})$, again by (v) and Lemma 4.12).

Let

$$\varphi'(v, \vec{a''}) \quad := \quad \exists w_0 \ldots \exists w_m (\wedge_{i \leq m} p_i(w_0, \ldots, w_i, \vec{a''}) \wedge \varphi(v, \vec{w}, \vec{a''}).$$

Notice that the parameters in $\varphi'(v, \vec{a''})$ –including the coefficients of the p_i– are in F, and either transcendental over $K(\mathcal{F})$ or in $K(\mathcal{F})$, and in the latter case we can assume that they are in $Z(\mathcal{F})$ itself.
If our hypothesis is satisfied under the assumptions of Claim 1, then there is some $c \in F$ such that $\mathcal{C}$ satisfies $\varphi'(c, \vec{a''})$ and consequently $\varphi(c, \vec{r}, \vec{a''})$ for some suitable tuple $\vec{r}$. Note that $\vec{r}$ is in F. Also, there is an automorphism f of $\mathcal{C}$ such that:

a) f fixes $Z(\mathcal{C})$, and consequently $E(\mathcal{C})$, $K(\mathcal{C})$, pointwise and $K(\mathcal{C})^{alg}$ setwise,

b) in particular f fixes $Z(\mathcal{F})$, $E(\mathcal{F})$, $K(\mathcal{F})$ pointwise and $K(\mathcal{F})^{alg}$ setwise,

c) f maps $\vec{r}$ to $\vec{a'}$ and $\vec{a''}$ to itself,

d) finally $f(c) \in F$.

Then $\mathcal{C} \models \varphi(f(c), \vec{a})$. In this way our proposition is proved in the general case, that is, for an arbitrary $\vec{a}$, provided that it is true in the restricted case, when $\vec{a}$ is as in Claim 1.

Claim 2: We can assume that $\mathcal{C}$ is a big saturated model of T. Otherwise we replace $\mathcal{C}_F$ –the expansion of $\mathcal{C}$ by all the elements of F– by a big saturated elementary extension. It is easily seen that passing to this model preserves the conditions on $\mathcal{C}$.

We will continue our proof under the further assumptions given in Claims 1 and 2. Let $c \in C$ satisfy $\varphi(c, \vec{a})$. If c is transcendental over $K(\mathcal{C})(\vec{a''})$, then every element of C transcendental over $K(\mathcal{C})(\vec{a''})$ satisfies $\varphi(v, \vec{a})$ as well. If no element algebraic over $K(\mathcal{C})(\vec{a''})$ satisfies $\varphi(v, \vec{a})$, then

$$C - K(\mathcal{C})(\vec{a''})^{alg} = \varphi(\mathcal{C}, \vec{a})$$

is definable, as well as $K(\mathcal{C})(\vec{a''})^{alg}$. But this contradicts what was observed in Proposition 4.7, because $K(\mathcal{C})(\vec{a''})^{alg}$ is an algebraically closed proper subfield of C extending $K(\mathcal{C})$.
Thus we can assume that c is algebraic over $K(\mathcal{C})(\vec{a''})$.
Notice that $\varphi(v, \vec{a})$ is satisfied by any root of the minimal polynomial $p(x)$ of c over $K(\mathcal{C})(\vec{a''})$, as well as by the image of c under any automorphism of $\mathcal{C}$ fixing $\vec{a}$ pointwise. Without loss of generality we can assume that the coefficients of $p(x)$ are finite sums of monomials of the form $gl_1^{h_1} \ldots l_s^{h_s}$ where $(l_1, \ldots, l_s)$ is $\vec{a''}$ and g is in $Z(\mathcal{C})$. Let $\vec{M}$ denote the sequence of all the elements $g \in Z(\mathcal{C})$ obtained in this way. Observe that $\vec{M}$ enlarges $\vec{a'}$. Rearrange $\vec{M}$ to obtain an increasing sequence where the elements of $\vec{a'}$ come before those lying in $\vec{M}$ but not in $\vec{a'}$ (just replace each M in $\vec{M}$ but not in $\vec{a'}$ by $M + a$ where a is the coordinate of $\vec{a'}$ with the maximum value). Also we can arrange the elements lying in $\vec{M}$ but not in $\vec{a'}$, as $M_0 < M_1 < \ldots < M_k$ and suppose that all of them are non-standard. Let $M_0 = 1$ and assume that it belongs to $\vec{a'}$. For every sequence $\vec{M'}$ expanding $\vec{a'}$, with the same type as $\vec{M}$ in T (including EXP), there is an automorphism f of $\mathcal{C}$ sending $\vec{M}$ to $\vec{M'}$ that fixes $\vec{a'}$ pointwise and even $\vec{a''}$ pointwise (because $\vec{a''}$ is algebraically independent over $K(\mathcal{C})$). Consequently, $f(c)$ viewed as a root of the polynomial obtained by replacing $\vec{M}$ by $\vec{M'}$ in $p(x)$ still satisfies $\varphi(v, \vec{a})$. Actually by compactness, a finite part of the type of $\vec{M}$ in T is sufficient to imply $\varphi(v, \vec{a})$. By Proposition 5.1, a finite part of the type of $\vec{M}$ in the first order theory of the ring of integers is enough to do so. But this finite subset of the whole type of $\vec{M}$ can be also realized in $Z(\mathcal{F})$ (where $\mathbf{Z}$ and $\vec{a'}$ lie), and consequently in F, by some suitable tuple $\vec{M''}$. Recall that F is algebraically closed and includes $\vec{a''}$. Thus any root of the polynomial obtained by replacing $\vec{M}$ by $\vec{M''}$ in $p(x)$ is in F, and satisfies $\varphi(v, \vec{a})$. $\dashv$

Corollary 5.3 *$\mathcal{C}_0$ is elementarily embeddable in every model $\mathcal{C}$ of T. In particular $\mathcal{C}_0$ is a prime model of T.*

Proof. As observed in Lemma 4.10, the canonical embedding of $\mathcal{C}_0$ into $\mathcal{C}$ satisfies conditions (i) and (v). The further hypotheses of Proposition 5.2 are also satisfied. In particular $Z(\mathcal{C}_0) = \mathbf{Z}$ is an elementary substructure of $Z(\mathcal{C})$, and indeed a prime model of the theory of the ring of integers. $\dashv$

Theorem 5.4 *The theory T is complete, and hence equals the first order theory of ($\mathbf{C}$, $\mathbf{Z}$, exp).*

Proof. Every model of T is an elementary extension of $\mathcal{C}_0$, and so is elementarily equivalent to it. $\dashv$

References

[1] E. Casanovas, M. Ziegler, Stable theories with a new predicate, J. Symbolic Logic 66 (2001), 1127–1140

[2] J. Heidenreich, *Stability Theory modulo a Predicate*, Ph.D. Thesis, University of Notre Dame, 2005

[3] W. Hodges, *A shorter Model Theory*, Cambridge University Press, Cambridge, 1997

[4] J. Kirby, The Geometry of Schanuel's Conjecture, unpublished notes (see Kirby's website)

[5] K. Vozoris, *The Complex Field with a Predicate for the Integers*, Ph.D. Thesis, University of Illinois at Chicago, 2007

[6] A. 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. 9 (1996), 1051–1094

[7] B. Zilber, Pseudo-exponentiation on algebraically closed fields of characteristic 0, Ann. Pure Applied Logic 132 (2004), 67–95