On Schanuel's Conjecture

Petra Staynova

September 12, 2012

Acknowledgements. I would like to thank my Supervisor, Dr. Jonathan Pila, for the many hours spent in supervision and e-mails, patience while I learned the basics, and constant encouragement and support since the beginning of this Dissertation. He has been a true source of inspiration and a very good listener.

Contents

1 Introduction

1.1 Overview of This Dissertation

Schanuel's Conjecture has a cornucopia of interesting consequences, from such intuitive, but surprisingly yet unproven, statements, like the algebraic independence of the numbers e, e^{π}, e^{e}, e^{i} to deep model-theoretic results, like the decidability of the real field with exponentiation [20]. Several fundamental theorems of Transcendental Number Theory are partial cases of Schanuel's Conjecture. One major part of this Dissertation is devoted to proving in detail the Lindemann-Weierstraß Theorem.

In Section 1, we provide basic definitions and results we take for granted.

In Section 2, we state the conjecture and give some preliminary consequences, which may be conjectures or known results.

In Section 3, we consider four Theorems, which are at the heart of Transcendental Number Theory: the Lindemann-Weierstraß Theorem, the Gel'fond-Schneider Theorem, Baker's Theorem, and the Six Exponentials Theorem. Each is considered in some sense an improvement of the previous ones, and the proofs respectively grow in complexity. We provide a proof of the first and last of these, highlighting our main contribution to this project throughout the exposition, and outline the middle two. We completely restructure the proof of the Lindemann-Weierstraß Theorem in hopes of making the main ideas more transparent and easily seen; to this aim, we needed to adapt several of the auxiliary propositions from the literature, and formulate several different from the ones found in the literature used. Our proof of the LW Theorem follows from the exposition in [6], which uses only the basic notions of Complex and Real Analysis and thus is accessible to undergraduate students. Our main contribution consists of restructuring the proof presented in [6] and correcting various omissions, inaccuracies, and errors, which of course do not affect the natural approach of making this proof more transparent and accessible.

In Section 4, we provide two very interesting consequences of Schanuel's Conjecture, and survey several other fascinating corollaries.

Finally, in Section 5, we provide applications of Schanuel's Conjecture in Model Theory, with the most important two being a (very brief) overview of Zilber's pseudoexponentiation, and the decidability of the real field with exponentiation under Schanuel's Conjecture.

1.2 Some Notation, Definitions, and Preliminary Results

Principle. [6] The Fundamental Principle of (Transcendental) Number Theory states that there is no integer $\mathcal{N}$ satisfying $0 < \mathcal{N} < 1$.

1.1 Notation. If X is any set and $M \in \mathbb{N}^{+}$, then $[X]^{M}$ denotes the set of all subsets of X consisting of exactly M different elements, i.e.

$$[X]^{M} = \{A : A \subset X : |A| = M\}.$$

1.2 Notation. We use the following standard notations:

- $\mathbb{N}$ for the natural numbers (0 is included in $\mathbb{N}$)
- $\mathbb{N}^{+}$ for the positive natural numbers
- $\mathbb{Z}$ for the integers
- $\mathbb{Q}$ for the rational numbers
- $\mathbb{R}$ for the real numbers

- $\mathbb{C}$ for the complex numbers
- $\mathrm{Re}(z)$ for the real part of $z \in \mathbb{C}$
- $\mathrm{Im}(z)$ for the imaginary part of $z \in \mathbb{C}$
- $\overline{\mathbb{Q}}$ for the set of algebraic numbers
- If K is a field, $K[z_1, \ldots, z_n]$ denotes the ring of all polynomials in n variables $z_1, \ldots, z_n$ and with coefficients in K
- If $p(z) = a_n z^n + \ldots + a_1 z + a_0 \in \mathbb{Z}[z]$ we say that $p(z)$ is a polynomial in variable z with integer coefficients. When $a_n = \ldots = a_0 = 0$, we call the polynomial the zero polynomial.

1.3 Definition. If $a_n \neq 0$ we say that the *degree* of $p(z)$ is n, and a_n is called the *leading coefficient* of $p(z)$. We write $\deg(p) = n$. If $a_n = 1$, then $p(z)$ is called *monic*.

1.4 Definition. A number $\alpha \in \mathbb{C}$ is called *algebraic* if it is a zero of some nonzero polynomial $p(z) \in \mathbb{Z}[z]$, or equivalently, the zero of a nonzero polynomial with rational coefficients. We call $\alpha \in \mathbb{C}$ an *algebraic integer* if moreover the polynomial $p(z)$ is monic.

1.5 Definition. A polynomial $p(z) \in \mathbb{Z}[z]$ (alternatively - in $\mathbb{Q}[z]$) is called *irreducible* if it cannot be factored into two polynomials in $\mathbb{Z}[z]$ (or $\mathbb{Q}[z]$), each having a strictly smaller degree than $p(z)$.

1.6 Theorem. *[28] If $\alpha \in \overline{\mathbb{Q}}$ then there is a unique monic irreducible (over $\mathbb{Q}$) polynomial $f \in \mathbb{Q}[z]$ satisfying $f(\alpha) = 0$.*

1.7 Definition. We call the above polynomial $p(z)$ the *minimal polynomial of* α. We define the *degree of* α, denoted $\deg(\alpha)$, to be $\deg(p)$.

1.8 Definition. If $\alpha \in \overline{\mathbb{Q}}$, we define the *conjugates of* α to be the zeros in $\mathbb{C}$ of the minimal polynomial of α.

1.9 Note. Some basic facts about algebraic numbers:

1. The set $\overline{\mathbb{Q}}$ is countable (this follows from the countability of $\mathbb{Z}$);
2. $\overline{\mathbb{Q}}$ contains the set $\{p + iq : p, q \in \mathbb{Q}\}$,
3. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, this implies that $\overline{\mathbb{Q}}$ is dense in $\mathbb{C}$.

1.10 Theorem. *[28] The set $\overline{\mathbb{Q}}$ with the operations of complex addition, subtraction, multiplication and division is a field.*

1.11 Definition. [18] Any field L containing the field K, is called a *field extension* of K, and denoted by $L \supset K$. If $L \supset K$ and $\alpha \in L \setminus K$, we can define a field extension $K(\alpha)$ of K as the smallest subfield of L containing K and α, and denote it by $K(\alpha)$. We say that the field $K(\alpha)$ is a field extension of K generated by α. If $\alpha_1, \ldots, \alpha_n \in L \setminus K$, we can analogously define $K(\alpha_1, \ldots, \alpha_n)$, and it can be shown that $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1)(\alpha_2, \ldots, \alpha_n) = \ldots = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.

1.12 Example. The complex numbers $\mathbb{C}$ are an extension field of the real numbers $\mathbb{R}$, generated by i; in other words, $\mathbb{C} = \mathbb{R}(i)$. The field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is the subfield of $\mathbb{R}$, generated by $\sqrt{2}$ over $\mathbb{Q}$.

1.13 Definition. [27] Let $L \supseteq K$ be a field extension and $\{a_1, \ldots, a_n\} \subset L$. We say that $a_1, \ldots, a_n$ are *algebraically dependent over* K if there exists a nonzero polynomial $f \in K[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$. We say that $a_1, \ldots, a_n$ are *aglebraically independent over* K if they are not algebraically dependent.

1.14 Definition. (paraphrase from [27]) Let $L \supset K$ be a field extension. We say that a subset $\{a_1, \ldots, a_n\} \in L$ is a *transcendence basis* of L over K if the following properties hold:

1. $a_1, \ldots, a_n$ are algebraically independent over K,
2. if $\beta \in L$, then β is algebraic over the field $K(a_1, \ldots, a_n)$.

It is fairly standard to show that

1.15 Proposition. *[18] If $L \supset K$ and $a_1, \ldots, a_n, b_1, \ldots, b_m \in L$ are such that both $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_m\}$ are maximal algebraically independent sets, then $m = n$.*

Hence, we are justified in making the following definition, in analogy to basis of a vector field:

1.16 Definition. The *transcendence degree* of a set S over a field K, denoted $\mathrm{trdeg}_K(S)$, is the size of the maximal subset S' of S such that S' is algebraically independent.

Or, alternatively,

1.17 Definition. The *transcendence degree* of a field extension L over K, denoted by $\mathrm{trdeg}_K(L)$, is the cardinality of any transcendence basis of L over K.

1.18 Proposition. *[27] If $L = K(a_1, \ldots, a_n)$, then $trdeg_K(L) \leqslant n$, and there exists a subset of $\{a_1, \ldots, a_n\}$ which is a transcendence basis of $L \supset K$.*

1.19 Note. [27] For $a_1, \ldots, a_n \in \mathbb{C}$, we have

$$\mathrm{trdeg}_{\mathbb{Q}}(\mathbb{Q}(a_1, \ldots, a_n)) = \mathrm{trdeg}_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}(a_1, \ldots, a_n))$$

1.20 Note. If the field K is clear, we will often drop the subscript 'K' in $\mathrm{trdeg}_K(L)$ and respectively 'over K' in our exposition.

2 A First Look at Schanuel's Conjecture

2.1 Conjecture (Schanuel's Conjecture)**.** *[27] Let $x_1, \ldots, x_n$ be complex numbers linearly independent over $\mathbb{Q}$. Then*

$$trdeg_{\mathbb{Q}}(\mathbb{Q}(x_1, \ldots, x_n, e^{x_1}, e^{x_2}, \ldots, e^{x_n})) \geqslant n.$$

Equivalently, one may state Schanuel's Conjecture as:

2.2 Conjecture (Schanuel's Conjecture)**.** *If $x_1, \ldots, x_n$ are $\mathbb{Q}$-linearly independent complex numbers, then among the $2n$ numbers $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$, at least n are algebraically independent over $\mathbb{Q}$.*

This conjecture includes a plethora of consequences, many of which are other conjectures we would like to believe to be true, and others are well-known results.

2.1 Theorems, Which are Consequences of Schanuel's Conjecture

Taking $n = 1$ in Schanuel's Conjecture, or SC for short, we get

2.3 Theorem (Hermite-Lindemann [13], [34]). *If $x \in \mathbb{C} \setminus \{0\}$, then at least one of x, e^x is transcendental.*

As immediate consequences of this Theorem, we get:

2.4 Proposition. *The following numbers are transcendental:*

1. *e (taking $x = 1$),*
2. *π (by contradiction - if $\pi \in \overline{\mathbb{Q}}$, then $i\pi \in \overline{\mathbb{Q}}$ so both of $i\pi, e^{i\pi} = -1 \in \overline{\mathbb{Q}}$),*
3. *$\log 2$ ($x = \log 2$),*
4. *$e^{\sqrt{2}}$ ($x = \sqrt{2} \in \overline{\mathbb{Q}}$).*

The case when $x_1, \ldots, x_n \in \overline{\mathbb{Q}}$ is:

2.5 Theorem (Lindemann-Weierstraß). *If $x_1, \ldots, x_n \in \overline{\mathbb{Q}}$ are $\mathbb{Q}$-linearly independent, then the numbers $e^{x_1}, \ldots, e^{x_n}$ are $\mathbb{Q}$-algebraically independent.*

Though this is an immediate consequence of Schanuel's Conjecture, the proof of this theorem was a major breakthrough in Transcendental Number Theory, and all existing proofs are long and strenuous - Section 3.1 is devoted to the detailed proof of this theorem, and much more.

Also, the solution to Hilbert's seventh problem (discussed in Section 3.2) is a consequence of Schanuel's Conjecture:

2.6 Theorem (Gel'fond-Schneider). *If $\alpha, \beta \in \overline{\mathbb{Q}} \setminus \{0\}$, $\alpha \neq 1$, and $\beta \notin \mathbb{Q}$, then any value of α^β is transcendental.*

Baker's Theorem, the crown jewel of 20th century Transcendental Number Theory, also follows from Schanuel's Conjecture:

2.7 Theorem (Baker's Theorem). *If $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ and $\log \alpha_1, \ldots, \log \alpha_n$ are $\mathbb{Q}$-linearly independent, then the numbers $1, \log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over $\overline{\mathbb{Q}}$.*

The Six Exponentials Theorem is another Corollary of Schanuel's Conjecture:

2.8 Theorem (Six Exponentials). *Let $x_1, x_2 \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$, and let $y_1, y_2, y_3 \in \mathbb{C}$ also be linearly independent over $\mathbb{Q}$. Then at least one of the six numbers*

$$e^{y_1 x_1}, e^{y_1 x_2}, e^{y_2 x_1}, e^{y_2 x_2}, e^{y_3 x_1}, e^{y_3 x_2}$$

is transcendental (over $\mathbb{Q}$).

In Section 3.4 we provide a proof and historical background of the Six Exponentials Theorem.

2.2 Consequences of Schanuel's Conjecture Which are Conjectures

By an easy induction on n, one can use Schanuel's Conjecture to obtain the algebraic independence of

$$e+\pi, e\pi, \pi^e, e^e, e^{e^2}, \ldots, e^{e^e}, \ldots, \pi^\pi, \pi^{\pi^2}, \ldots, \pi^{\pi^\pi}, \ldots$$

and of

$$\log\pi, \log(\log 2), \pi\log 2, (\log 2)(\log 3), 2^{\log 2}, (\log 2)^{\log 3}, \ldots.$$

Even the case when $n=2$ of Schanuel's Conjecture is not yet known:

2.9 Conjecture. *If $x_1, x_2 \in \mathbb{C}$ are $\mathbb{Q}$-linearly independent, then at least 2 of the 4 numbers $x_1, x_2, e^{x_1}, e^{x_2}$ are algebraically independent.*

An immediate consequence is the algebraic independence of:

1. e and π ($x_1 = 1, x_2 = i\pi$);
2. e and e^e ($x_1 = 1, x_2 = e$);
3. π and e^π ($x_1 = \pi, x_2 = i\pi$);
4. $\log 2$ and $\log 3$ ($x_1 = \log 2, x_2 = \log 3$);
5. $\log 2$ and $2^{\log 2}$ ($x_1 = \log 2, x_2 = (\log 2)^2$).

To give an idea of the difficulty of these seeminly innocuous consequences, item 3 was not proven until 1996:

2.10 Theorem (Nesterenko)**.** *[24] π and e^π are algebraically independent.*

We also don't know if there exist two logaritms of algebraic numbers which are algebraically independent - a more general version of item 4 above. In this vein, we have the Four Exponentials Conjecture, which is a generalisation of the Six Exponentials Theorem:

2.11 Conjecture (Four Exponentials)**.** *Given $\alpha_1, \ldots, \alpha_4 \in \mathbb{C}$ such that $(\log\alpha_1)(\log\alpha_4) = (\log\alpha_2)(\log\alpha_3)$, then either $\log\alpha_1$ and $\log\alpha_2$ are linearly dependent, or else $\log\alpha_1$ and $\log\alpha_3$ are linearly dependent.*

An alternative statement of the conjecture is:

2.12 Conjecture (Four Exponentials)**.** *[38] If $\alpha_1, \alpha_2, \beta_2, \beta_2 \in \mathbb{C}$ are such that α_1, α_2 are linearly independent over $\mathbb{Q}$ and β_1, β_2 are $\mathbb{Q}$-linearly independent, then at least one of the four numbers*

$$e^{\alpha_1\beta_1}, e^{\alpha_1\beta_2}, e^{\alpha_2\beta_1}, e^{\alpha_2\beta_2},$$

is transcendental.

An interesting corollary of the Four Exponentials Conjecture is:

2.13 Corollary. *If for some $\alpha \in \mathbb{C}$, both $2^\alpha \in \mathbb{N}$ and $3^\alpha \in \mathbb{N}$, then $\alpha \in \mathbb{N}$.*

This leads the author to pose the following question:

Open Question. If $3^\alpha - 2^\alpha \in \mathbb{N}$ for $\alpha \in \mathbb{C}$, can we deduce that either $\alpha \in \mathbb{N}$ or $\alpha \in \mathbb{C} \setminus \overline{\mathbb{Q}}$?

2.14 Proposition (the author's)**.** *Schanuel's Conjecture implies that if $3^\alpha - 2^\alpha \in \mathbb{N}$, then $\alpha \in \mathbb{Q}$ or $\alpha \in \mathbb{C} \setminus \overline{\mathbb{Q}}$.*

Proof. Assume Schanuel's Conjecture and consider the set $\{\log 2, \log 3, \alpha \log 2, \alpha \log 3\}$ for $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$. This set is $\mathbb{Q}$-linearly independent, so by SC,

$$\operatorname{trdeg}_{\mathbb{Q}}(\mathbb{Q}(\log 2, \log 3, \alpha \log 2, \alpha \log 3, 2, 3, 2^{\alpha}, 3^{\alpha})) \geqslant 4.$$

Noting that

$$\mathbb{Q}(\log 2, \log 3, \alpha \log 2, \alpha \log 3, 2, 3, 2^{\alpha}, 3^{\alpha}) = \mathbb{Q}(\log 2, \log 3, 2^{\alpha}, 3^{\alpha})$$

and applying Proposition 1.18, we have

$$\operatorname{trdeg}_{\mathbb{Q}}(\mathbb{Q}(\log 2, \log 3, 2^{\alpha}, 3^{\alpha})\}) = 4.$$

Hence, $3^{\alpha} - 2^{\alpha}$ is transcendental for α algebraic irrational.

By the contrapositive, we have that if $3^{\alpha} - 2^{\alpha} \in \mathbb{N}$, then α cannot be algebraic irrational, so $\alpha \in \mathbb{Q}$ or $\alpha \in \mathbb{C} \setminus \overline{\mathbb{Q}}$. □

Another vaguely related question is:

Open Question. For $A \subseteq \mathbb{R}$ and $f(x) = 2^x$, when do we have that $f(A) \subseteq A$?

Clearly this holds for:

1. $A = \mathbb{R}$;
2. $A = \mathbb{N}$;
3. $A = [a, \infty)$ for any $a \in \mathbb{R}$;
4. more generally, for any A built inductively by taking $A_0 = \{a\}$ and $A_{n+1} = \{2^b : b \in A_n\}$, and setting $A = \cup_{n \in \mathbb{N}} A_n$, for $a \in \mathbb{R}$ arbitrary;
5. for arbitrary unions of sets of the form in item 4.

But are there any other subsets of $\mathbb{R}$ for which this holds? Can we prove that no other such subsets exist, given Schanuel's Conjecture?

Gel'fond (in 1948) and Schneider (in 1952) conjectured that:

2.15 Conjecture. *If $\alpha, \beta \in \overline{\mathbb{Q}}$ and if β has degree $d \geqslant 2$, then $trdeg_{\mathbb{Q}}\left(\mathbb{Q}\left(\alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}}\right)\right) = d - 1$.*

A straightforward proof of Conjecture assuming Schanuel's Conjecture can be found in in [27].

2.16 Note. For parts of this subsection, we used material from [35] and [14].

3 Four Important Theorems

3.1 The Lindemann-Weierstraß Theorem

This section is devoted to proving the important partial case of Schanuel's Conjecture, the Lindemann-Weierstraß Theorem 2.5. We first list three equivalent versions of the Lindemann-Weierstraß Theorem:

3.1 Theorem (Lindemann-Weierstraß - first version[4])**.** *Let $\{\alpha_0, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}}]^{M+1}$. Then the numbers $e^{\alpha_0}, \ldots, e^{\alpha_M}$ are linearly independent over $\overline{\mathbb{Q}}$.*

It is easy to check that Theorem 3.1 is equivalent to:

3.2 Theorem (Lindemann-Weierstraß - second version)**.** *If $\alpha_0, \alpha_1, \ldots, \alpha_M \in \overline{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$. Then the numbers $e^{\alpha_0}, e^{\alpha_1}, \ldots, e^{\alpha_M}$ are $\mathbb{Q}$-algebraically independent.*

Since the algebraic independence of complex numbers over $\mathbb{Q}$ is equivalent to linear independence over $\overline{\mathbb{Q}}$, Theorem 3.1 is also equivalent to:

3.3 Theorem (Lindemann-Weierstraß - third version)**.** *If $\{\alpha_0, \alpha_1, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}}]^{M+1}$, then $e^{\alpha_0}, \ldots, e^{\alpha_M}$ are $\overline{\mathbb{Q}}$-linearly independent.*

First let us consider a very natural question: what does the Lindemann-Weierstraß theorem have to do with transcendental numbers? How was it arrived at? In other words, what does the linear independence of $\{e^{\alpha_0}, \ldots, e^{\alpha_M}\}$ over $\overline{\mathbb{Q}}$ have to do with transcendence?

To answer this question, let us recall the previously mentioned Hermite's theorem (also known as Lindemann's Theorem, or the Hermite-Lindemann Theorem):

3.4 Theorem (Hermite's Theorem [13])**.** *The number e^{α} is transcendental for any $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$.*

In fact, Hermite's Theorem states that if $\alpha \neq 0$ and β are algebraic numbers, then $e^{\alpha} \neq \beta$. So, it can be restated as:

3.5 Theorem. *If $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$ and $\beta_0, \beta_1 \in \overline{\mathbb{Q}}$ are not both zero, then $\beta_0 e^0 + \beta_1 e^{\alpha} \neq 0$.*

In other words, $\{e^0, e^{\alpha}\}$ are $\overline{\mathbb{Q}}$-linearly independent. The Lindemann-Weierstraß Theorem is a natural generalization of this result: if $\{\alpha_0, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}}]^{M+1}$ then $\{e^{\alpha_0}, \ldots, e^{\alpha_M}\}$ is $\overline{\mathbb{Q}}$-linearly independent.

We shall provide a proof of the first version of the Lindemann-Weierstraß Theorem 3.1.

There are four major approaches in proving the Lindemann-Weierstraß Theorem. The two most recent methods use Galois Theory and extension fields ([25]), and a criterion of rationality for solutions of linear differential equations ([5]). The third one is the Weierstraß approach [41], using integrals of the type $\int p_m(z) e^z dz$; such a proof can be found in [4]. The fourth one can be found in [6] (the proof given in [10] is essentially the same). All proofs of the Lindemann-Weierstraß Theorem are proofs by contradiction, and are based on constructing an integer $\mathcal{N}$ that is between 0 and 1 and thus violating the Fundamental Principle of Transcendental Number Theory. The definition of such an integer initially involves an arbitrary prime p that later can be used in two essential ways: firstly, to ensure that $\mathcal{N}$ is nonzero, and consequently, to make $\mathcal{N}$ between 0 and 1.

The proof of Lindemann-Weierstraß presented here takes the fourth approach from those listed above. It uses results from Complex Analysis, prevailingly the concept of conjugates, the Taylor Series of e^z and some fundamental limits from Real Analysis. In general, we follow [6], but we completely restructure the proof in hopes of clarifying it. We base our proof on 3 key new Lemmas: 3.17, 3.19, and 3.20. Another contribution of our presentation is to correct a couple of errors that occur in the proof given in [6]. The first one is a false statement which is key to proving that the integer $\mathcal{N}$ in question is nonzero. This concerns the way in which the first choice of the prime p is made. In [6], the authors choose $p > A^p$, where $A \geqslant 1$. Obviously, this is impossible, except in some trivial cases, because the exponential function A^x is always greater than x for $A > 1$. Among other contributions are formulating lemmas and defining notions in a more rigorous manner, so they can be legitimately applied later in the proof. Unfortunately, this cannot be done with some of the main lemmas in [6], for example [6, Challenge 3.11, pg 66], stated without proof, since the preconditions are not met when the challenge is later used. We also provide detailed proofs of statements only formulated in the form of Challenges.

First, we need some more definitions.

3.6 Definition. $S \in [\mathbb{Q}]^M$ is called a *complete set of conjugates* if whenever $\alpha \in S$, all conjugates of α are in S.

3.7 Definition. $A = \{\alpha_1, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}} \setminus \{0\}]^M$ is called a *complete collection of conjugates* if A consists of all the zeros of the polynomial (factored in $\mathbb{C}$)

$$h(z) = (z - \alpha_1)(z - \alpha_2) \ldots (z - \alpha_M) \in \mathbb{Q}[z].$$

Thus $h(z)$ is the minimal polynomial over $\mathbb{Q}$ of each of the α_m's.

3.8 Definition. If $A = \{\alpha_1, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}} \setminus \{0\}]^M$ is a complete set of conjugates, we say that A *splits into* L *complete collections of conjugates* if A can be written as

$$A_1 = \{\alpha_{11}, \ldots, \alpha_{1M_1}\}, \ldots, A_l = \{\alpha_{l1}, \ldots, \alpha_{lM_l}\}, \ldots, A_L = \{\alpha_{L1}, \ldots, \alpha_{LM_L}\},$$

where each A_l is a complete collection of conjugates.

Now we proceed with some preliminaries to the proof of the Lindemann-Weierstraß Theorem.

The usual approach is firstly to prove the following special case and then conclude the general result from it:

3.9 Theorem. *Let $\{\alpha_1, \alpha_2, \ldots, \alpha_M\}$ be a complete set of conjugates. Let $\{\beta_0, \beta_1, \ldots, \beta_M\} \subset \mathbb{Z} \setminus \{0\}$ be such that if α_i and α_j are conjugates then $\beta_i = \beta_j$. Then*

$$\beta_0 + \sum_{m=1}^{M} \beta_m e^{\alpha_m} = \beta_0 + \beta_1 e^{\alpha_1} + \ldots + \beta_M e^{\alpha_M} \neq 0.$$

We base our proof on the interplay between the so-called auxilliary polynomial, defined on the basis of $\alpha_1, \ldots, \alpha_M$, and the Taylor series of e^z. Firstly, we construct a nonzero integer $\mathcal{N}$ in such a way that it is closely connected to a special partial sum of the Taylor series of e^z, choosing the prime p in a special manner. Then, we further improve our choice of the prime p to make the corresponding tail arbitrarily small. Finally, assuming for a contradiction that the conclusion of Theorem 3.9 is not true, we link $\mathcal{N}$, the tail, and the auxilliary polynomial to make $\mathcal{N}$ violate the Fundamental Principle of Transcendental Number Theory.

We list some basic results from Algebra concerning symmetric polynomials that will be needed for the proof.

3.10 Definition. Let $F(x_1, \ldots, x_L)$ be a function of L variables. We say that F is a *symmetric function* if any permutation of the variables does not change the function.

3.11 Fact. The sum and the product of two symmetric functions in n variables is also a symmetric function.

A simple procedure for generating symmetric polynomials in L unknowns is to look at $x_1, \ldots, x_L$ as zeros of a polynomial in z and then consider the coefficients of that polynomial:

$$F(z) = (z - x_1)(z - x_2) \ldots (z - x_L) = z^L - \sigma_1 z^{L-1} + \sigma_2 z^{L-2} - \ldots + (-1)^L \sigma_L,$$

where the $\sigma_1, \ldots, \sigma_L$ are the symmetric polynomials generated by Viète's formulas:

- $\sigma_1(x_1, \ldots, x_L) = x_1 + \ldots + x_L$
- $\sigma_2(x_1, \ldots, x_L) = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{L-1}x_L$

- ...
- $\sigma_L(x_1, \ldots, x_L) = x_1 x_2 \ldots x_L$.

3.12 Definition. We call $\sigma_1, \ldots, \sigma_L$ *elementary* symmetric polynomials, or *elementary symmetric functions* in $x_1, \ldots, x_L$ and often denote them by $\sigma_1, \ldots, \sigma_L$ only.

They are called elementary because any other symmetric polynomial with rational coefficients can be expressed as a polynomial in $\sigma_1, \ldots, \sigma_L$.

Here we shall prove the following lemma:

3.13 Lemma. *Let $G(z) = a_L z^L + a_{L-1} z^{L-1} + \ldots + a_1 z + a_0 \in \mathbb{Z}[z]$ be of degree L. Let $\{\alpha_1, \ldots, \alpha_L\}$ be all the zeros of $G(z)$. Then for every $i \in \{1, \ldots, L\}$, we have that $\sigma_i(\alpha_1, \ldots, \alpha_L)$ is a rational number with denominator a_L.*

3.14 Note. We note that:

1. The elementary symmetric polynomials $\sigma_1, \ldots, \sigma_L$ are in fact functions from $\mathbb{C}^L \to \mathbb{C}$.
2. Hence what is meant by the conclusion of this Lemma is that the *values* of σ_i at the point $(\alpha_1, \ldots, \alpha_L) \in \mathbb{C}^L$, where $\alpha_1, \ldots, \alpha_L$ are all the zeros of $G(z)$, are rational numbers with denominator a_L.
3. $G(z)$ might be irreducible over $\mathbb{Z}[z]$ but if we factor it in $\mathbb{C}[z]$, we get $G(z) = a_L(z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_L)$. Then $\{\alpha_1, \ldots, \alpha_L\}$ is either a complete set of conjugates (if G is irreducible over $\mathbb{Z}$) or a collection of complete sets of conjugates, each corresponding to the set of zeros of the irreducible over $\mathbb{Z}$ factors of G.

Proof. By the Fundamental Theorem of Algebra, $G(z)$ splits over $\mathbb{C}$ in linear factors as:

$$G(z) = a_L(z - \alpha_1)(z - \alpha_1)\ldots(z - \alpha_L)$$

and, according to our definition of the σ_i's, the right hand side of the above equation is equal to

$$a_L \left(z^L - \sigma_1(\alpha_1, \ldots, \alpha_L) z^{L-1} + \sigma_2(\alpha_1, \ldots, \alpha_L) z^{L-2} + \ldots + (-1)^L \sigma_L(\alpha_1, \ldots, \alpha_L)\right).$$

Also

$$G(z) = a_L z^L + \ldots + a_0 = a_L \left(z^L + \frac{a_{L-1}}{a_L} z^{L-1} + \ldots + \frac{a_1}{a_L} z + \frac{a_0}{a_L}\right).$$

Equating the two expressions for $G(z)$, we get

$$\begin{aligned} &a_L \left(z^L + \frac{a_{L-1}}{a_L} z^{L-1} + \ldots + \frac{a_1}{a_L} z + \frac{a_0}{a_L}\right) \\ &= a_L \left(z^L - \sigma_1(\alpha_1, \ldots, \alpha_L) z^{L-1} + \sigma_2(\alpha_1, \ldots, \alpha_L) z^{L-2} + \ldots + (-1)^L \sigma_L(\alpha_1, \ldots, \alpha_L)\right) \end{aligned}$$

By comparing coefficients in front of corresponding powers of z we get:

$$\begin{aligned} \sigma_1 = \alpha_1 + \ldots + \alpha_L &= -\frac{a_{L-1}}{a_L} \\ \sigma_1 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{L-1}\alpha_L &= \frac{a_{L-2}}{a_L} \\ \vdots &\quad \vdots \\ \sigma_1 = \alpha_1 \ldots \alpha_L &= (-1)^L \frac{a_0}{a_L} \end{aligned}$$

and obviously all values at the right hand side are rational numbers (since the a_i's are integers).

□

3.15 Lemma. *Let $G(z), \mathcal{P}(z) \in \mathbb{Z}[z]$, $\deg G(z) = L$, $G(z) = a_L z^L + a_{L-1} z^{L-1} + \ldots + a_1 z + a_0$ and let $\{\alpha_1, \ldots, \alpha_L\}$ denote all the zeros of $G(z)$. Then the number*

$$\mathcal{P}(\alpha_1) + \mathcal{P}(\alpha_2) + \ldots + \mathcal{P}(\alpha_L)$$

is a rational number with denominator equal to $a_L^{\deg(\mathcal{P})}$.

3.16 Note. Instead of following the approach in [6], which uses further results about symmetric polynomials, here we provide a more direct proof of this Lemma.

Proof. Let $\mathcal{P}(z) = b_0 + b_1 z + b_2 z^2 + \ldots + b_n z^n$ and $\deg \mathcal{P}(z) = n$. Define

$$\begin{aligned} B(\alpha_1, \ldots, \alpha_L) &= \mathcal{P}(\alpha_1) + \mathcal{P}(\alpha_2) + \ldots + \mathcal{P}(\alpha_L) \\ &= (b_0 + b_1\alpha_1 + \ldots + b_n\alpha_1^n) + \ldots + (b_0 + b_1\alpha_L + \ldots + b_n\alpha_L^n) \\ &= Lb_0 + b_1(\alpha_1 + \ldots + \alpha_L) + b_2(\alpha_1^2 + \ldots + \alpha_L^2) + \ldots + b_n(\alpha_1^n + \ldots + \alpha_L^n), \end{aligned}$$

which is evidently a symmetric polynomial in $(\alpha_1, \ldots, \alpha_L)$. Let us consider the expression

$$H_i(\alpha_1, \ldots, \alpha_L) = \alpha_1^i + \alpha_2^i \ldots + \alpha_L^i.$$

If we complete H_i to $(\alpha_1 + \ldots + \alpha_L)^i$, for $i = 1, \ldots, n$, then we see that $B(\alpha_1, \ldots, \alpha_L)$ can be expressed as a polynomial with integer coefficients in the elementary symmetric polynomials $\sigma_1, \ldots, \sigma_L$ in $(\alpha_1, \ldots, \alpha_L)$, and hence we can rewrite B as

$$B(\alpha_1, \ldots, \alpha_L) = F(\sigma_1, \ldots, \sigma_L) \in \mathbb{Z}[\sigma_1, \ldots, \sigma_L],$$

where evidently $\deg F \leqslant \deg B$. By Lemma 3.13, each $\sigma_k(\alpha_1, \ldots, \alpha_L)$ is a rational number with denominator a_L. Hence the expression $F(\sigma_1, \ldots, \sigma_L)$ is a rational number with denominator $a_L^{\deg F}$. But $\deg F \leqslant \deg B$ and $\deg B = \deg \mathcal{P}$. Hence there is $A \in \mathbb{Z}$ such that

$$\begin{aligned} B(\alpha_1, \ldots, \alpha_L) = F(\sigma_1, \ldots, \sigma_L) &= \frac{A}{a_L^{\deg F}} \\ &= \frac{A a_L^{\deg B - \deg F}}{a_L^{\deg F} a_L^{\deg B - \deg F}} \\ &= \frac{A}{a_L^{\deg B}} a_L^{\deg B - \deg F} \\ &= \frac{C}{a_L^{\deg \mathcal{P}}}, \end{aligned}$$

where $C = A.a_L^{\deg B - \deg F} \in \mathbb{Z}$. □

As part of our restructuring of the proof, we formulate and prove the following new lemma:

3.17 Lemma. *For a given complete set of conjugates $\{\alpha_1, \ldots, \alpha_M\} \in [\mathbb{Q} \setminus \{0\}]^M$ that splits into L complete collections of conjugates*

$$\{\alpha_{11}, \ldots, \alpha_{1M_1}\}, \ldots, \{\alpha_{l1}, \ldots, \alpha_{lM_l}\}, \ldots, \{\alpha_{L1}, \ldots, \alpha_{LM_L}\}$$

and a prime number p, we can define integers $\{d_l, a_l, D = d_1 \dots d_L, c_N : l = 1, \dots, L; N = p-1, p, \dots, (M+1)p-1\}$ where in addition $c_{p-1} \neq 0$, $d_l > 0$, and a_l is divisible by p for $l = 1, \dots, L$. We also define a polynomial $\mathcal{P}_p(z)$ of degree $Mp-1$ such that

$$\sum_{m=1}^{M_l} \frac{\mathcal{P}_p(\alpha_{lm})}{(p-1)!} = \frac{a_l}{d_l^{Mp-1}},$$

for $l = 1, \dots, L$.

Proof. For every $\{\alpha_{l1}, \dots, \alpha_{lM_l}\}$, let $f_l(z) \in \mathbb{Q}[z]$ be its minimal polynomial, ie.

$$f_l(z) = (z - \alpha_{l1})(z - \alpha_{l2}) \dots (z - \alpha_{lM_l}).$$

Then there is $d_l \in \mathbb{Z}^+$ such that $g_l(z) = d_l f_l(z) \in \mathbb{Z}[z]$ and $\deg g_l = \deg f_l = M_l$ for $l = 1, \dots, L$. Let $D = d_1 d_2 \dots d_L$, so $D \in \mathbb{Z}^+$. Define a polynomial

$$f(z) = D^p z^{p-1} f_1(z)^p f_2(z)^p \dots f_L(z)^p = z^{p-1} g_1(z)^p g_2(z)^p \dots g_L(z)^p,$$

so

$$\deg f = p - 1 + M_1 p + M_2 p + \dots M_L p = p(1 + M_1 + M_2 + \dots + M_L) - 1 = (M+1)p - 1,$$

and the smallest degree of z in $f(z)$ is $p-1$. Since $D \in \mathbb{Z}^+$ and $g_l \in \mathbb{Z}[z]$, $l = 1, \dots, L$, we have that $f(z) \in \mathbb{Z}[z]$. We rewrite $f(z)$ as:

$$f(z) = \sum_{n=p-1}^{(M+1)p-1} c_n z^n,$$

where $c_n \in \mathbb{Z}$ for $n = p-1, p, p+1, \dots, (M+1)p-1$. By Viete's formulas,

$$c_{p-1} = \pm D^p (\alpha_1 \dots \alpha_M)^p \in \mathbb{Z} \setminus \{0\}.$$

Define the polynomial $\mathcal{P}_p(z)$ as:

$$\mathcal{P}_p(z) = \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=0}^{N-p} \frac{z^n}{n!} \right),$$

where by convention the inner sums for $N = p-1$ and $N = p$ are defined to be zero. In expanded form, this gives us

$$\mathcal{P}_p(z) = (p+1)! c_{p+1} \sum_{n=0}^{1} \frac{z^n}{n!} + (p+2)! c_{p+2} \sum_{n=0}^{2} \frac{z^n}{n!} + \dots + c_{(M+1)p-1}((M+1)p-1)! \sum_{n=0}^{Mp-1} \frac{z^n}{n!} =$$

(this is a polynomial with integer coefficients with respect to the partial sums of the Taylor expansion of e^z up to $Mp-1$)

$$= (p+1)! c_{p+1}(1+z) + (p+2)! c_{p+2}(1 + z + \frac{z^2}{2!}) + \dots +$$
$$+ ((M+1)p-1) c_{(M+1)p-1} \left(1 + z + \frac{z^2}{2!} + \dots + \frac{z^{Mp-1}}{(Mp-1)!}\right)$$

We can rewrite $\mathcal{P}_p(z)$ as:

$$\mathcal{P}_p(z) = p!\Big((p+1)c_{p+1}(1+z) + (p+1)(p+2)c_{p+2}(1+z+\frac{z^2}{2!}) + \\ \ldots + (p+1)(p+2)\ldots(p+Mp-1)c_{(M+1)p-1}(1+z+\frac{z^2}{2!}+\ldots+\frac{z^{Mp-1}}{(Mp-1)!})\Big).$$

Since $p+1, p+2, \ldots, p+Mp-1$ are $Mp-1$ consecutive integers, their product is divisible by $(Mp-1)!$ (a simple fact from modular arithmetic is that $(p+1)(p+2)\ldots(p+n)$ is divisible by $n!$). Hence $\mathcal{P}_p(z) = p!$(a polynomial with integer coefficients), i.e. $\frac{1}{p!}\mathcal{P}_p(z) \in \mathbb{Z}[z]$.

Recalling that $\{\alpha_{l1}, \ldots, \alpha_{lM_l}\}$ are all the zeros of $g_l(z)$ for each $l = 1, \ldots, L$, we apply Lemma 3.15 to $\frac{1}{p!}\mathcal{P}_p(z)$ and $g_l(z)$. For a particular l we have:

$$\frac{1}{p!}(\mathcal{P}_p(\alpha_{l1}) + \mathcal{P}_p(\alpha_{l2}) + \ldots + \mathcal{P}_p(\alpha_{lM_l})) = \sum_{m=1}^{M_l} \frac{\mathcal{P}_p(\alpha_{lm})}{p!} = \frac{a_l'}{d_l^{Mp-1}}, \tag{1}$$

for some $a_l' \in \mathbb{Z}$; recall that $\deg \mathcal{P}_p(z) = Mp-1$ and $d_l \in \mathbb{Z}^+$ is the leading coefficient of $g_l(z)$. Now let $a_l = pa_l'$ and rewrite (1) as

$$p\sum_{m=1}^{M_l} \frac{\mathcal{P}_p(\alpha_{lm})}{p!} = \frac{a_l}{d_l^{Mp-1}},$$

where $a_l \in \mathbb{Z}$ and is divisible by p, or

$$\sum_{m=1}^{M_l} \frac{\mathcal{P}_p(\alpha_{lm})}{(p-1)!} = \frac{a_l}{d_l^{Mp-1}}. \tag{2}$$

Thus we have defined the required integers $D, c_{p-1}, c_N, d_l, a_l$ and the polynomial $\mathcal{P}_p(z)$ for $l = 1, \ldots, L$ and $N = p-1, p, p+1, \ldots, (M+1)p-1$. □

3.18 Note. We reserve the right to use some of the polynomials and intermediate results given above whenever applicable in the consequent exposition.

The key step in our restructuring of the proof of the Lindemann-Weierstraß Theorem is the definition of the nonzero integer $\mathcal{N}$.

3.19 Lemma. *Let $\{\alpha_1, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}} \setminus \{0\}]^M$ be a complete set of conjugates that splits into L complete collections of conjugates*

$$\{\alpha_{11}, \ldots, \alpha_{1M_1}\}, \ldots, \{\alpha_{l1}, \ldots, \alpha_{lM_l}\}, \ldots, \{\alpha_{L1}, \ldots, \alpha_{LM_L}\}.$$

Let $\{\beta_0, \ldots, \beta_M\} \subset \mathbb{Z} \setminus \{0\}$ be such that if α_i and α_j are conjugates, then $\beta_i = \beta_j$. Then there is a prime number p such that the number

$$\mathcal{N} = \beta_0 D^{Mp} c_{p-1} + \left(\beta_0 D^{Mp} \sum_{N=p}^{(M+1)p-1} \frac{N!}{(p-1)!} c_N + \sum_{l=1}^{L} a_l \beta_l d_l \left(\frac{D}{d_l}\right)^{Mp}\right),$$

where $\{D, d_l, a_l, c_N : l = 1, \ldots, L; N = p-1, p, \ldots, (M+1)p-1\}$ are as in Lemma 3.17, is a nonzero integer.

Proof. $\mathcal{N}$ *is an integer:*

Evidently, $\frac{D}{d_l} \in \mathbb{Z}^+$ for $l = 1, \ldots, L$. Also, $\sum_{N=p}^{(M+1)p-1} c_N \frac{N!}{(p-1)!}$ is an integer divisible by p, since for $N = p, p+1, \ldots, (M+1)p-1$ we have that

$$\frac{N!}{(p-1)!} = \frac{p(p-1)!N_p}{(p-1)!},$$

where $N_p \in \mathbb{N}^+$. Hence $\mathcal{N}$ is indeed an integer. By our choice of a_l's, it follows that $\sum_{l=1}^{L} a_l \beta_l d_l \left(\frac{D}{d_l}\right)^{Mp}$ is an integer divisible by p.

$\mathcal{N}$ *is nonzero:*

We have $\beta_0 D^{Mp} c_{p-1} \neq 0$. Hence, in order to show that $\mathcal{N} \neq 0$, it is enough to show that p can be chosen such that $\beta_0 D^{Mp} c_{p-1}$ is not divisible by p.

According to [6], page 61, p can be chosen to be $p > \max\{|\beta_0|, |c_{p-1}|, D\}$. However, since $|c_{p-1}| = |\alpha_1 \ldots \alpha_M d_1 \ldots d_l|^p$, this can be done only in the case when $\max\{|\beta_0|, |c_{p-1}|, D\} = 1$, which is a very special case since all of them are integers, $\{d_1, \ldots, d_l\}$ are integers, and that would mean in particular that $|\beta_0| = 1$, $D = 1$, and hence $d_1 = d_2 = \ldots = 1$ and $|\alpha_1 \ldots \alpha_M| = 1$. For all other non-trivial choices of β_0 and $\alpha_1, \ldots, \alpha_M$ we would have that $\max\{|\beta_0|, |c_{p-1}|, D\} \geqslant |\alpha_1 \ldots \alpha_M d_1 \ldots d_l|^p$ and $|\alpha_1 \ldots \alpha_M d_1 \ldots d_l| > 1$. Hence we cannot choose p in such a manner, since the linear function $F(x) = x$ grows slower than the exponential function A^x for $A = |\alpha_1 \ldots \alpha_M d_1 \ldots d_l| > 1$, i.e. for $A > 1$, $A^x > x$ for all real x.

We will amend the book's proof in the following way: the divisors of $\beta_0 D^{Mp} c_{p-1}$ are exactly the divisors of β_0, D, and c_{p-1}, and are finitely many, and hence bounded above. By the Archimedean Principle, there is a positive integer $\mathfrak{P}$ greater than the absolute value of each of them. Since the set of prime numbers is not bounded above in $\mathbb{N}$, we can choose our prime $p > \mathfrak{P}$. Then $\beta_0 D^{Mp} c_{p-1}$ will be a nonzero integer not divisible by p.

Hence $\mathcal{N}$ is a nonzero integer. □

It doesn't come as a surprise that in Lemma 3.17 we have defined the polynomial $\mathcal{P}_p(z)$ as a polynomial in the partial sums of the Taylor expansion of e^z,

$$\mathcal{P}_p(z) = \sum_{N=p-1}^{(M+1)p-1} N! c_N \sum_{n=0}^{N-p} \frac{z^n}{n!}.$$

Lemmas 3.17 and 3.19 will be used in the proof of a special case of the Lindemann-Weierstraß Theorem, where we will encounter some linear combinations of values of e^z in given algebraic numbers $\{\alpha_1, \ldots, \alpha_M\}$. We will aim to show that the prime number p can be further "enlarged" so that the nonzero integer $\mathcal{N}$, defined in Lemma 3.19 can be made to violate the Fundamental Principle of Transcendental Number Theory. In order to do that, we will bound it above by some quantity that for sufficiently "large" primes p can be made smaller than 1. One very good candidate in the way of obtaining such a quantity is the corresponding sum (finite - from $p-1, p, \ldots, p+Mp-1$) of the corresponding tails of the series for e^z.

The following Lemma is given as Challenge 3.10 [6, pg 61] without proof; our proof here uses the natural approach explored in [7], but we completely rework the proof, correcting various inaccuracies.

3.20 Lemma. *Let p be a prime number and $\{\alpha_1, \ldots, \alpha_M\}$, c_N $(N = p-1, \ldots, p+Mp-1)$, be as in Lemma 3.17. Let us consider the finite sum of the tails of the Taylor expansion of e^z:*

$$\mathcal{T}_p(z) = \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{z^n}{n!} \right).$$

Then there are two constants K_1 and K_2 that do not depend on p such that for any $\alpha \in \{\alpha_1, \ldots, \alpha_M\}$,

$$|\mathcal{T}_p(\alpha)| \leqslant K_1 (K_2)^p.$$

Proof.

$$\begin{aligned}
\mathcal{T}_p(z) &= \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{z^n}{n!} \right) \\
&= \sum_{N=p-1}^{(M+1)p-1} \left(c_N \sum_{n=N}^{\infty} \frac{N! z^n}{n!} \right) \\
&= \sum_{N=p-1}^{(M+1)p-1} \left(c_N \sum_{n=0}^{\infty} \frac{N! z^{n+N}}{(n+N)!} \right),
\end{aligned}$$

so

$$\begin{aligned}
|\mathcal{T}_p(\alpha)| &\leqslant \sum_{N=p-1}^{(M+1)p-1} |c_N| \left| \sum_{n=0}^{\infty} \frac{N! \alpha^{n+N}}{(n+N)!} \right| \\
&\leqslant \sum_{N=p-1}^{(M+1)p-1} |c_N| \sum_{n=0}^{\infty} \frac{N!}{(n+N)!} |\alpha|^n |\alpha|^N \\
&= \sum_{N=p-1}^{(M+1)p-1} |c_N| |\alpha|^N \sum_{n=0}^{\infty} \frac{N!}{(n+N)!} |\alpha|^n \qquad \left(\text{because } \frac{N!}{(N+n)!} \leqslant \frac{1}{n!} \right) \\
&\leqslant \sum_{N=p-1}^{(M+1)p-1} |c_N| |\alpha|^N \sum_{n=0}^{\infty} \frac{|\alpha|^n}{n!} \\
&= e^{|\alpha|} \sum_{N=p-1}^{(M+1)p-1} |c_N| |\alpha|^N \qquad (3)
\end{aligned}$$

If $|\alpha| \leqslant 1$, we have

$$(3) \leqslant e^{|\alpha|} \sum_{N=p-1}^{(M+1)p-1} |c_N|,$$

and if $|\alpha| \geqslant 1$, we have

$$(3) = e^{|\alpha|} \left(|c_{p-1}| |\alpha|^{p-1} + |c_p| |\alpha|^p + \ldots + |c_{(M+1)p-1}| |\alpha|^{(M+1)p-1} \right).$$

Hence

$$(3) \leqslant e^{|\alpha|} |\alpha|^{(M+1)p-1} \sum_{N=p-1}^{(M+1)p-1} |c_N|.$$

Since when $|\alpha| \leqslant 1$, the proof can be easily completed, we shall proceed with the case when $|\alpha| \geqslant 1$. Recall that c_N, $N = p-1, \ldots, (M+1)p-1$ were the integer coefficients of

$$f(z) = D^p z^{p-1}(z-\alpha_1)^p(z-\alpha_2)^p \ldots (z-\alpha_M)^p.$$

For each $m = 1, \ldots, M$, by the Binomial formula, we have

$$(z-\alpha_m)^p = \sum_{k=0}^{p} \binom{p}{k} (-\alpha_m)^{p-k} z^k.$$

Let us find an upper bound for the coefficients of $(z-\alpha_m)^p$ that does not depend on m. We have

$$\begin{aligned}
\max_{k=0,1,\ldots,p} \left\{ \left| \binom{p}{k} (-\alpha)^p \right| \right\} &\leqslant \sum_{k=0}^{p} \binom{p}{k} |\alpha|^{p-k} \\
&\leqslant |\alpha|^p \sum_{k=0}^{p} \binom{p}{k} \\
&= 2^p |\alpha|^p \\
&(2|\alpha|)^p,
\end{aligned}$$

where, again the more complicated case is when $|\alpha| \geqslant 1$. We proceed with this assumption in mind. Hence each coefficient in $(z-\alpha)^p$ is bounded above by $(2|\alpha|)^p$ and we have M such factors in $f(z)$. Hence

$$|c_N| \leqslant D^p (2|\alpha|)^{Mp}.$$

Hence

$$\sum_{N=p-1}^{(M+1)p-1} |c_N| \leqslant D^p (2|\alpha|)^{Mp} Mp.$$

Hence

$$\begin{aligned}
|\mathcal{T}_p(\alpha)| &\leqslant e^{|\alpha|} |\alpha|^{(M+1)p-1} D^p (2|\alpha|)^{Mp} Mp \\
&= \frac{e^{|\alpha|}}{|\alpha|} D^p Mp ((2|\alpha|)^M)^p (|\alpha|^{M+1})^p \\
&\underset{\substack{M \in \mathbb{Z}^+ \\ Mp \leqslant M^p}}{\leqslant} \frac{e^{|\alpha|}}{|\alpha|} D^p M^p ((2|\alpha|)^M)^p (|\alpha|^{M+1})^p.
\end{aligned}$$

Now defining $K_1 = \frac{e^{|\alpha|}}{|\alpha|}$ and $K_2 = DM2^M |\alpha|^{2M+1}$, we obtain the required result. □

The following Lemma is Challenge 2.4 from [6], given without proof:

3.21 Lemma. *Let $p(z) = z^j(z-a)^{j+1}$ for some integer $j \geqslant 1$. Then $\sum_{n=1}^{j} f^{(n)}(a) = 0$.*

Proof. We rewrite $p(z)$ as $p(z) = \sum_{n=j}^{2j+1} a_n z^n$. Since a is a zero of $p(z)$ of multiplicity $j+1$ and $\deg p(z) > j+1$, a will be a zero of all the derivatives of $p(z)$ up to j, i.e. $p'(a) = p''(a) = \ldots = p^{(j)}(a) = 0$ □

Now note that, for $1 \leqslant n \leqslant p-1$, the nth derivative $f^{(n)}$of our $f(z) = \sum_{n=p-1}^{(M+1)p-1} c_n z^n \in \mathbb{Z}[z]$ can be written in closed form as

$$f^{(n)}(z) = \sum_{N=p-1}^{(M+1)p-1} \frac{N!}{(N-n)!} c_N z^{N-n}.$$

This helpful remark allows us to prove:

3.22 Lemma. *For $f(z)$ we have that*

$$\sum_{n=1}^{p-1} f^{(n)}(z) = \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right)$$

Proof.

$$\begin{aligned}
\sum_{n=1}^{p-1} f^{(n)}(z) &= \sum_{n=1}^{p-1} \left(\sum_{N=p-1}^{(M+1)p-1} \frac{N!}{(N-n)!} c_N z^{N-n} \right) \\
&= \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=1}^{p-1} \frac{z^{N-n}}{(N-n)!} \right) \\
&= \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right)
\end{aligned}$$

□

Now, let us proceed to the proof of a special case of the Lindemann-Weierstraß, from which we shall deduce the general statement of the Theorem.

3.23 Theorem. *Let $\{\alpha_1, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}} \setminus \{0\}]^M$ be a complete set of conjugates, let $\{\beta_0, \beta_1, \ldots, \beta_M\} \in \mathbb{Z} \setminus \{0\}$ be such that if α_i and α_j are conjugates then $\beta_i = \beta_j$. Then*

$$\beta_0 + \beta_1 e^{\alpha_1} + \ldots + \beta_M e^{\alpha_M} \neq 0.$$

Proof. Let $A = \{\alpha_1, \ldots, \alpha_M\}$ split into

$$\{\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1M_1}\},\ \{\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2M_2}\},\ \ldots,\ \{\alpha_{L1}, \alpha_{L2}, \ldots, \alpha_{LM_L}\},$$

and let $d_l, a_l, D = d_1 \ldots d_L, c_N, f_l(z), g_l(z)$, for $l = 1, \ldots, L$ and $N = p-1, p, \ldots, (M+1)p-1$, and $p, f(z), \mathcal{P}_p(z)$ be as in Lemma 3.17, and let $\mathcal{T}_p(z)$ be as in Lemma 3.20.

Suppose, for a contradiction, that there are $\beta_1, \ldots, \beta_M \subset \mathbb{Z} \setminus \{0\}$ such that $\beta_i = \beta_j$ whenever α_i and α_j are conjugates and

$$\beta_0 + \beta_1 e^{\alpha_1} + \ldots + \beta_M e^{\alpha_M} = 0. \tag{4}$$

Since $\beta_i = \beta_j$ whenever α_i and α_j are conjugates, we can re-index the β_i's accordingly. In this way, β_l will be the coefficient corresponding to the complete collection of conjugates $\{\alpha_{l1}, \ldots, \alpha_{lM_l}\}$, i.e. $\beta_l = \beta_{l1} = \beta_{l2} = \ldots = \beta_{lM_l}$, where β_{lm} is the coefficient of $e^{\alpha_{lm}}$ for $l = 1, \ldots, L$ and $m = 1, \ldots, M_L$. Now we may rewrite (4) as

$$\beta_0 + \sum_{l=1}^{L} \beta_l \left(e^{\alpha_{l1}} + e^{\alpha_{l1}} + \ldots + e^{\alpha_{lM_l}} \right) = \beta_0 + \sum_{l=1}^{L} b_l \left(\sum_{m=1}^{M_l} e^{\alpha_{lm}} \right) = 0 \tag{5}$$

By Lemma 3.22 applied to our polynomial $f(z)$, we get

$$\sum_{n=1}^{p-1} f^{(n)}(z) = \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right) \tag{6}$$

The sum in the inner brackets of (6) is part of the power series of e^z. This leads us to relate it to our α's from $\{\alpha_1, \ldots, \alpha_M\}$ and for each $\alpha \in \{\alpha_1, \ldots, \alpha_M\}$ to consider the expression

$$\sum_{N=p-1}^{(M+1)p-1} N! c_N e^{\alpha} = \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} \right) = \text{we split the 'inner' power series into three parts:}$$

one before the RHS of (6) + RHS of (6) + the tail of the power series after the RHS of (6)

$$= \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=0}^{N-p} \frac{\alpha^n}{n!} \right) + \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{\alpha^n}{n!} \right) + \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{\alpha^n}{n!} \right).$$

The sum in the middle is exactly the right-hand side of (6) evaluated at α and, by Lemma 3.21, is equal to zero. Hence

$$\begin{aligned} e^{\alpha} \sum_{N=p-1}^{(M+1)p-1} N! c_N &= \sum_{N=p-1}^{(M+1)p-1} N! c_N e^{\alpha} \\ &= \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=0}^{N-p} \frac{\alpha^n}{n!} \right) + \sum_{N=p-1}^{(M+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{\alpha^n}{n!} \right) \\ &= \mathcal{P}_p(\alpha) + \mathcal{T}_p(\alpha) \end{aligned} \tag{7}$$

i.e.

$$e^{\alpha} \sum_{N=p-1}^{(M+1)p-1} N! c_N = \mathcal{P}_p(\alpha) + \mathcal{T}_p(\alpha). \tag{8}$$

Now we multiply both sides of the identity (5) by $N! c_N / (p-1)!$ and get

$$\frac{N! c_N}{(p-1)!} \left(\beta_0 + \sum_{l=1}^{L} \beta_l \left(\sum_{m=1}^{M_l} e^{\alpha_{lm}} \right) \right) = 0. \tag{9}$$

Letting N vary from $p-1$ to $(M+1)p-1$, we obtain Mp such identities, which we sum up:

$$\sum_{N=p-1}^{(M+1)p-1} \left(\frac{N! c_N}{(p-1)!} \left(\beta_0 + \sum_{l=1}^{L} \beta_l \left(\sum_{m=1}^{M_l} e^{\alpha_{lm}} \right) \right) \right) = 0, \tag{10}$$

or, after expanding a bit and switching the three sum symbols we get

$$\frac{\beta_0}{(p-1)!} \sum_{N=p-1}^{(M+1)p-1} N! c_N + \frac{1}{(p-1)!} \sum_{l=1}^{L} \beta_l \left(\sum_{m=1}^{M_l} e^{\alpha_{lm}} \sum_{N=p-1}^{(M+1)p-1} N! c_N \right) = 0 \tag{11}$$

We now evaluate (8) in $\alpha = \alpha_{lm}$ and obtain

$$e^{\alpha_{lm}} \sum_{N=p-1}^{(M+1)p-1} N! c_N = \mathcal{P}_p(\alpha_{lm}) + \mathcal{T}_p(\alpha_{lm}). \tag{12}$$

From (11) and (12) we obtain by substitution:

$$\frac{\beta_0}{(p-1)!}\sum_{N=p-1}^{(M+1)p-1} N!c_N + \frac{1}{(p-1)!}\sum_{l=1}^{L}\beta_l\sum_{m=1}^{M_l}\left(\mathcal{P}_p(\alpha_{lm})+\mathcal{T}_p(\alpha_{lm})\right)=0, \tag{13}$$

and writing the 'tail' part to the right we get

$$\frac{\beta_0}{(p-1)!}\sum_{N=p-1}^{(M+1)p-1} N!c_N + \frac{1}{(p-1)!}\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\mathcal{P}_p(\alpha_{lm})\right)=-\frac{1}{(p-1)!}\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\mathcal{T}_p(\alpha_{lm})\right) \tag{14}$$

Putting $\frac{1}{(p-1)!}$ inside the sum, we get

$$\beta_0\sum_{N=p-1}^{(M+1)p-1}\frac{N!c_N}{(p-1)!} + \sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\frac{\mathcal{P}_p(\alpha_{lm})}{(p-1)!}\right)=-\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right) \tag{15}$$

Recalling equality (2):

$$\sum_{m=1}^{M_l}\frac{\mathcal{P}_p(\alpha_{lm})}{(p-1)!}=\frac{a_l}{d_l^{Mp-1}},$$

and by substituting it in (15) we get

$$\beta_0\sum_{N=p-1}^{(M+1)p-1}\frac{N!c_N}{(p-1)!} + \sum_{l=1}^{L}\beta_l\frac{a_l}{d_l^{Mp-1}}=-\sum_{l=1}^{L}\beta_l\left(\sum_{m=1}^{M_l}\frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right). \tag{16}$$

Now we multiply both sides of (16) by D^{Mp} to obtain

$$\beta_0 D^{Mp}\sum_{N=p-1}^{(M+1)p-1}\frac{N!c_N}{(p-1)!} + \sum_{l=1}^{L}\beta_l\frac{a_l}{d_l^{Mp-1}}D^{Mp}=-\sum_{l=1}^{L}\beta_l D^{Mp}\left(\sum_{m=1}^{M_l}\frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right). \tag{17}$$

We can rewrite the left-hand side of (17) and get

$$\beta_0 D^{Mp}c_{p-1}+\beta_0 D^{Mp}\sum_{N=p}^{(M+1)p-1}\frac{N!c_N}{(p-1)!} + \sum_{l=1}^{L}\beta_l a_l d_l\left(\frac{D}{d_l}\right)^{Mp}=-\sum_{l=1}^{L}\beta_l D^{Mp}\left(\sum_{m=1}^{M_l}\frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right). \tag{18}$$

Recalling Lemma 3.19, (18) is in fact:

$$\mathcal{N}=-\sum_{l=1}^{L}\beta_l D^{Mp}\left(\sum_{m=1}^{M_l}\frac{\mathcal{T}_p(\alpha_{lm})}{(p-1)!}\right), \tag{19}$$

and we remind the reader that $\mathcal{N}$ is a nonzero integer. Taking the absolute value of both sides of (19) and applying the triangle inequality finitely many times, we get

$$0<|\mathcal{N}|<\sum_{l=1}^{L}\left(\sum_{m=1}^{M_l}\frac{|\beta_l|D^{Mp}|\mathcal{T}_p(\alpha_{lm})|}{(p-1)!}\right). \tag{20}$$

Let $B = \max\{|\beta_1|, |\beta_2|, \ldots, |\beta_L|\}$. Then from Lemma 3.20 and (20) we get

$$\begin{aligned} 0 < |\mathcal{N}| &< \sum_{l=1}^{L} \left(\sum_{m=1}^{M_l} \frac{BD^{Mp} K_1 (K_2)^p}{(p-1)!} \right) \\ &= \frac{BD^{Mp} K_1 (K_2)^p}{(p-1)!} \sum_{l=1}^{L} \left(\sum_{m=1}^{M_l} 1 \right) \\ &= \frac{BD^{Mp} K_1 (K_2)^p}{(p-1)!} \sum_{l=1}^{L} M_l \\ &= \frac{BD^{Mp} K_1 (K_2)^p}{(p-1)!} \sum_{l=1}^{L} M_l \\ &= BMK_1 \frac{(D^M K_2)^p}{(p-1)!}. \end{aligned} \tag{21}$$

In short, (21) becomes

$$0 < |\mathcal{N}| < BMK_1 \frac{(D^M K_2)^p}{(p-1)!}. \tag{22}$$

The constants BMK_1 and $D^M K_2$ do not depend on p. We recall that

$$\lim_{p \to \infty} \frac{a^p}{(p-1)!} = 0, \tag{23}$$

hence the right hand side of (22) can be made smaller than 1 for sufficiently large primes p. So, for such p, we have that

$$0 < |\mathcal{N}| < 1, \tag{24}$$

which is the required contradiction with the Fundamental Principle of Transcendental Number Theory.

Hence, $\beta_0 + \sum_{m=1}^{M} \beta_m e^{\alpha_m} \neq 0$.

□

3.24 Definition. The finite subset $S \subset \overline{\mathbb{Q}}$ is called *conjugate-complete* if for all $\alpha \in S$, S contains all the conjugates of α and if α appears m times in S, then each conjugate of α appears m times in S, as well.

Note the difference between this definition, and Definition 3.6. Obviously any conjugate-complete set is a complete set of conjugates, but the converse doesn't always hold:

3.25 Example. The set $\{i\sqrt{5}, i\sqrt{5}, -i\sqrt{5}, -i\sqrt{5}, 3, \sqrt{7}, -\sqrt{7}\}$ is conjugate-complete, while $\{i\sqrt{5}, i\sqrt{5}, -i\sqrt{5}, 3, \sqrt{7}, -\sqrt{7}\}$ is not conjugate-complete, since we don't have two copies of $-i\sqrt{5}$, but is nonetheless a complete set of conjugates.

We shall define the following general notion:

3.26 Definition. The expression $\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \ldots + \beta_K e^{\alpha_K}$ is called a *conjugate-complete exponential sum* if $\{\alpha_1, \ldots, \alpha_K\}$ is conjugate-complete, where $\{\beta_1, \ldots, \beta_K\} \subset \mathbb{C}$.

In [6], the notion of conjugate complete exponential sum is used when $\beta_1 = \beta_2 = \ldots = \beta_K = 1$. Here we call this a conjugate-complete *simple* exponential sum:

3.27 Definition. The expression $e^{\alpha_1} + e^{\alpha_2} + \ldots + e^{\alpha_K}$ is called *a conjugate-complete simple exponential sum* if $\{\alpha_1, \ldots, \alpha_K\}$ is conjugate-complete (in the sense of Definition 3.24).

Next, we shall formulate and prove a new statement (Lemma 3.29), which is a more general version of [6, Challenge 3.11]. For that purpose, we will need the notion of a lexicographic order:

3.28 Definition. [12] Given a Cartesian product $X \times Y$ of two totally ordered sets X and Y, the *lexicographic order* of $X \times Y$ is: $(x_1, y_1) < (x_2, y_2)$ if and only if either

1. $x_1 < x_2$, or
2. $x_1 = x_2$ and $y_1 < y_2$.

When considering the lexicographic order in $\mathbb{C}$, we identify $\mathbb{C}$ with $\mathbb{R} \times \mathbb{R}$.

We will also need:

3.29 Lemma. *Let* $\{\rho_1, \ldots, \rho_L\} \in [\mathbb{C}]^L$, *let* $\{\tau_1, \ldots, \tau_M\} \in [\mathbb{C}]^M$ *and* $\{\tau_1, \ldots, \tau_L, t_1, \ldots, t_M\} \subset \mathbb{C} \setminus \{0\}$. *Then*

$$(r_1 e^{\rho_1} + \ldots + r_L e^{\rho_L})\,(t_1 e^{\tau_1} + \ldots + t_M e^{\tau_M}) = s_1 e^{\lambda_1} + \ldots + s_N e^{\lambda_N}$$

for some $N \in \mathbb{N}^+$ *and* $\{\lambda_1, \ldots, \lambda_N\} \in [\mathbb{C}]^N$. *In addition, at least one of* $\{s_1, \ldots, s_N\}$ *is nonzero.*

3.30 Note. In the formulation of Challenge 3.11, a stronger requirement is posed - namely - that $\{\rho_1, \ldots, \rho_L, \tau_1, \ldots, \tau_M\} \in [\mathbb{C}]^{L+M}$. Here we show that our more general form is still true, and, moreover, exactly this form will be used in the proof of the Lindemann-Weierstraß Theorem, since Challenge 3.11 is not applicable in the cases used in that proof.

Proof.

$$(r_1 e^{\rho_1} + \ldots + r_L e^{\rho_L})\,(t_1 e^{\tau_1} + \ldots + t_M e^{\tau_M}) = \sum_{l=1}^{L} \sum_{m=1}^{M} r_l t_m e^{\rho_l + \tau_m}$$

This expression has at most LM terms. Let $\lambda_{lm} = \rho_l + \tau_m$ and $s_{lm} = r_l t_m$ for $l = 1, \ldots, L$ and $m = 1, \ldots, M$. It might be that for some $(l', m'), (l'', m'') \in (L \times M)^2$, we have $\lambda_{l'm'} = \lambda_{l''m''}$, for example if $\rho_{l'} = -\tau_{m'}$ and $\rho_{l''} = -\tau_{m''}$.

We end up with N different λ_{lm}'s (the case when $N = 1$ and all $\lambda_{lm} = 0$ is not excluded - this might happen when $M = L$ and $\rho_l = -\tau_l$ for all $l = 1, \ldots, L$). We enumerate the λ_{lm}'s as $\lambda_1, \ldots, \lambda_N$. The corresponding coefficients $c_n, n = 1, \ldots, N$ will be sums of the s_{lm}'s that are coefficients of equal λ_{lm}'s.

We now prove that $\{c_1, \ldots, c_N\} \cap (\mathbb{C} \setminus \{0\}) \neq \emptyset$. The finite set $\{\mathrm{Re}(\rho_1), \ldots, \mathrm{Re}(\rho_L)\} \subset \mathbb{R}$ has a maximal element a^*; let $\{\rho_{l_1}, \ldots, \rho_{l_K}\} \subseteq \{\rho_1, \ldots, \rho_L\}$ be such that $\mathrm{Re}(\rho_{l_i}) = a^*$ for $i = 1, \ldots, K$. The finite set of real numbers $\{\mathrm{Im}(\rho_{l_1}), \ldots, \mathrm{Im}(\rho_{l_K})\}$ has a maximal element b^*; Let $\rho_s \in \{\rho_{l_1}, \ldots, \rho_{l_K}\}$ be such that $\rho_s = a^* + ib^*$. Since all ρ_l's are different, this ρ_s is unique and ρ_s will be the maximal element of $\{\mathrm{Re}(\rho_1), \ldots, \mathrm{Re}(\rho_L)\} \times \{\mathrm{Im}(\rho_1), \ldots, \mathrm{Im}(\rho_L)\} \subset \mathbb{R} \times \mathbb{R}$ with respect to the lexicographic order. Similarly, let $\tau_t \in \{\tau_1, \ldots, \tau_M\}$ be the unique maximal element of $\{\mathrm{Re}(\tau_1), \ldots, \mathrm{Re}(\tau_M)\} \times \{\mathrm{Im}(\tau_1), \ldots, \mathrm{Im}(\tau_M)\}$ with respect to the lexicographic order and let $\tau_t = c^* + id^*$.

We claim that the coefficient of $e^{\rho_s + \tau_t}$ is nonzero. Indeed, since $\rho_s = a^* + ib^*$ and $\tau_t = c^* + id^*$, we cannot have that

$$\rho_s + \tau_t = \rho_{s'} + \tau_{t'} \tag{25}$$

for some $(s', t') \neq (s, t)$. If $\rho_{s'} = x_s + iy_s$ and $\tau_{t'} = x_t + iy_t$, equation (25) gives us

$$a^* + ib^* + c^* + id^* = x_s + iy_s + x_t + iy_t \tag{26}$$

so

$$(a^* - x_s + c^* - x_t) + i(b^* - y_s + d^* - y_t) = 0. \tag{27}$$

This is possible only if

$$a^* - x_s + c^* - x_t = 0 = b^* - y_s + d^* - y_t.$$

But $a^* - x_s + c^* - x_t$ is a sum of two nonnegative numbers. So it is zero only if they are both zero, i.e. $a^* = x_s$ and $c^* = x_t$. Similarly $b^* = y_s$ and $d^* = y_t$, i.e. $\rho_s = \rho_{s'}$ and $\tau_s = \tau_{s'}$. This contradicts the uniqueness of ρ_s and τ_t.

Hence the coefficient of $e^{\rho_s+\tau_t}$ is exactly $\rho_s\tau_t$ and since they are both nonzero, it is also nonzero. □

3.31 Lemma. *The set $\{\alpha_1, \ldots, \alpha_L\}$ is conjugate-complete if and only if the polynomial $(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_L)$ has rational coefficients.*

3.32 Note. This is [6, Challenge 3.12], stated without proof.

Proof. Let $\{\alpha_1, \ldots, \alpha_L\}$ be conjugate-complete. Rewrite it as K complete collections of conjugates (where possibly some of those collections might coincide - for example - if α_1 appears p times, then the collections of all its conjugates will appear p times).

$$\{\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1L_1}\}, \{\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2L_2}\}, \ldots, \{\alpha_{K1} \ldots, \alpha_{KL_K}\},$$

where $L_1 + \ldots + L_K = L$. Let $f_l(z) = (z - \alpha_{l1})(z - \alpha_{l2})\ldots(z - \alpha_{lK_l})$ be the minimal polynomial over $\mathbb{Q}$ of the complete collection of conjugates $\{\alpha_{11}, \ldots, \alpha_{lK_l}\}$. Then $f(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_L) = f_1(z)f_2(z)\ldots f_K(z)$ and is in $\mathbb{Q}[z]$.

Conversely, suppose that $f(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_L) \in \mathbb{Q}[z]$. Suppose for a contradiction, that $A = \{\alpha_1, \ldots, \alpha_L\}$ is not conjugate-complete; let $\{\alpha_{11}, \ldots, \alpha_{1K}\}$ be all the conjugates of α_1, and without loss of generality, let $\{\alpha_{11}, \ldots, \alpha_{1k}\}$ be not in A, i.e.

$$A = \{\alpha_{1(k+1)}, \ldots, \alpha_{1K}, \alpha_{K+1}, \alpha_{K+2}, \ldots, \alpha_L\},$$

and also without loss of generality, let $\{\alpha_{K+1}, \ldots, \alpha_L\}$ be conjugate complete.

In the previous part, we have shown that

$$g_K(z) = (z - \alpha_{K+1})(z - \alpha_{K+2})\ldots(z - \alpha_L) \in \mathbb{Q}[z]$$

Again, let $f_1(z) = (z - \alpha_{11})\ldots(z - \alpha_{1k})(z - \alpha_{1(k+1)})\ldots(z - \alpha_{1K})$ be the minimal polynomial of α_1 over $\mathbb{Q}$ or, equivalently, be the minimal polynomial of $\{\alpha_{11}, \ldots, \alpha_{1K}\}$, so $f_1(z) \in \mathbb{Q}[z]$. Then we have

$$f(z) = (z - \alpha_{1(k+1)})\ldots(z - \alpha_{1K})(z - \alpha_{K+1})\ldots(z - \alpha_L) \in \mathbb{Q}[z].$$

Then

$$f(z) = (z - \alpha_{1(k+1)})\ldots(z - \alpha_{1K})g_K(z)$$

and since $g_K(z) \in \mathbb{Q}[z]$, we have that $h_1(z) = (z - \alpha_{1(k+1)})\ldots(z - \alpha_{1K})$ must be with rational coefficients, i.e. $h_1(z) \in \mathbb{Q}[z]$. But $\deg h_1(z) < \deg f_1(z)$ - contradiction with the minimality of $f_1(z)$ over $\mathbb{Q}$. □

3.33 Lemma. *Let $\{a_1, \ldots, a_J\} \subset \mathbb{Z}$ and $\{\gamma_1, \ldots, \gamma_J\} \subset \overline{\mathbb{Q}}$. Then the set of all linear combinations of all conjugates of γ_j's with coefficients a_j's is conjugate complete.*

3.34 Note. This lemma gives us a way to construct a conjugate complete set on the basis of an arbitrary set of algebraic numbers.

Proof. Let

$$A = \{a_1\tau_1 + a_2\tau_2 + \ldots + a_J\tau_J : \forall j = 1, \ldots, J,\ \tau_j \text{ is a conjugate of } \gamma_j\}.$$

Note that we do not exclude the case when some γ_i is a conjugate of some γ_j for $i \neq j$. We shall use Lemma 3.31 to prove that A is conjugate complete.

Let $\{\gamma_{j1}, \ldots, \gamma_{jJ_j}\}$ be the set of all conjugates of γ_j, for $j = 1, \ldots, J$. Let

$$\begin{aligned} p(z) = &(z - (a_1\gamma_{11} + a_2\gamma_2 + \ldots + a_J\gamma_J))\,(z - (a_1\gamma_{12} + a_2\gamma_2 + \ldots + a_J\gamma_J))\ldots \\ &\ldots(z - (a_1\gamma_{1J_1} + a_2\gamma_2 + \ldots + a_J\gamma_J)) = \\ &= \prod_{\substack{\tau_j \text{ is a conjugate of } \gamma_j \\ j=1,\ldots,J}} (z - (a_1\tau_1 + a_2\tau_2 + \ldots + a_J\tau_J)). \end{aligned}$$

We can rewrite $p(z)$ as

$$p(z) = \prod_{\substack{\tau_j \text{ is a conjugate of } \gamma_j \\ \text{for } 2 \leqslant j \leqslant J}} q(z),$$

where

$$\begin{aligned} q(z) = &\\ &(z - (a_1\gamma_{11} + a_2\tau_2 + \ldots + a_J\tau_J))(z - (a_1\gamma_{12} + a_2\tau_2 + \ldots + a_J\tau_J))\ldots \\ &\ldots(z - (a_1\gamma_{1J_1} + a_2\tau_2 + \ldots + a_J\tau_J)) = \\ &= \prod_{i=1}^{J_1} \big((z - a_2\tau_2 - \ldots - a_J\tau_J) - a_1\gamma_{1i}\big), \end{aligned}$$

or if we define $y = z - a_2\tau_2 - \ldots - a_J\tau_J$,

$$q(z) = f(y) = \prod_{i=1}^{J_1}(y - a_1\gamma_{1i}) = y^n - \sigma_1 y^{n-1} + \ldots + (-1)^n\sigma_n,$$

where σ_i's are the elementary symmetric functions in all the conjugates of γ_1 and by Lemma 3.13, are rationals. Hence $f(y) \in \mathbb{Q}[y]$ and $q(z) \in \mathbb{Q}[z, \tau_2, \ldots, \tau_J]$. We do this for all of the τ_j's and obtain that $p(z) \in \mathbb{Q}[z]$, hence by Lemma 3.31, $p(z) \in \mathbb{Q}[z]$. Hence A is conjugate complete.

□

3.35 Lemma. *Let $\{a_1, \ldots, a_L, b_1, \ldots, b_M\} \subset \mathbb{C} \setminus \{0\}$ and let $a_1e^{\alpha_1} + a_2e^{\alpha_2} + \ldots + a_Le^{\alpha_L}$, and $b_1e^{\gamma_1} + \ldots + b_Me^{\gamma_M}$ be two conjugate complete exponential sums. Then their product is a conjugate complete exponential sum.*

Proof.

$$(a_1e^{\alpha_1} + \ldots + a_Le^{\alpha_L})(b_1e^{\gamma_1} + \ldots + b_Me^{\gamma_M}) = \sum_{\substack{1 \leqslant l \leqslant L \\ 1 \leqslant m \leqslant M}} a_lb_me^{\alpha_l + \gamma_m}$$

Then $\{a_lb_m : l = 1, \ldots, L; m = 1, \ldots, M\} \subset \mathbb{C} \setminus \{0\}$ and by Lemma 3.33, the set $\{\alpha_l + \gamma_m : l = 1, \ldots, L; m = 1, \ldots, M\}$ is conjugate complete. □

3.36 Corollary. *The product of two conjugate complete simple exponential sums is a conjugate complete simple exponential sum.*

3.37 Theorem (The Lindemann-Weierstraß Theorem)**.** *Let* $\{\alpha_0, \alpha_1, \ldots, \alpha_M\} \subset \overline{\mathbb{Q}}$ *and suppose that* $\{\beta_0, \beta_1, \ldots, \beta_{M+1}\} \subset \overline{\mathbb{Q}} \setminus \{0\}$*. Then* $\beta_0 e^{\alpha_0} + \ldots + \beta_M e^{\alpha_M} \neq 0$*.*

Proof. We prove the Theorem by contradiction.

Suppose

$$\beta_0 e^{\alpha_0} + \ldots + \beta_M e^{\alpha_M} = 0 \tag{28}$$

First let us note that on page 68, line 13 in [6], it is written that $\{\beta_0, \beta_1, \ldots, \beta_M\} \subset \overline{\mathbb{Q}}$ are "not all zero". The $\beta_0, \beta_1, \ldots, \beta_M$ have to be *all nonzero*, because that is the statement of the Lindemann-Weierstraß Theorem, and also to enable us to later apply Lemma 3.29, where such a requirement is essential.

The idea is to first transform the left-hand side of (28) into a linear combination of conjugate complete exponential sums. In [6], it is written that by multiplying (28) by "analogous expressions with the collection of exponents replaced by all possible combinations of their corresponding conjugates:

$$\prod_{\substack{\rho_m \text{ is a conjugate of } \alpha_m \\ m=0,\ldots,M}} (\beta_0 e^{\rho_0} + \beta_1 e^{\rho_1} + \ldots + \beta_M e^{\rho_M}) = 0"$$

and then applying Lemma 3.29 (in form of their Challenge 3.11), we can ensure that this will not convert the left-hand side into an expression for 0. But in order to correctly apply Challenge 3.11 for two such multiples, all the exponents have to be different, and this is obviously not the case since such a product could contain, for example, two multiples with exponents $\{\rho_0, \rho_1, \ldots, \rho_M\}$ and $\{\rho_0, \rho'_1, \ldots, \rho'_M\}$. So we have to apply the "amended" by us version of Challenge 3.11, proved as Lemma 3.29.

To ensure this can be correctly done, let us make one more observation: it is possible that some α_i is a conjugate of α_j for some $i \neq j$ in $\{\alpha_0, \alpha_1, \ldots, \alpha_M\}$. Then we would have a multiple with exponents $\{\alpha_i, \alpha_i = \alpha_j, \text{ all others}\}$. At first glance, even Lemma 3.29 is not applicable, but let us note that then such an expression is reduced to $\ldots(\beta_i + \beta_j)e^{\alpha_i} + \ldots$, and then we can reduce any expression of the type $\beta_0 e^{\rho_0} + \beta_1 e^{\rho_1} + \ldots + \beta_M e^{\rho_M}$ to the expression of the type $b_0 e^{\gamma_0} + \ldots + b_L e^{\gamma_L}$, where $\{\gamma_0, \ldots, \gamma_L\} \in [\overline{\mathbb{Q}}]^L$ and $\{b_0, \ldots, b_L\}$ are integer linear combinations of β_m's and $\gamma_0, \ldots, \gamma_L$ are conjugates of some of $\{\alpha_0, \ldots, \alpha_M\}$. Lemma 3.29 can now be properly applied and we obtain an expression of the type

$$\sum_{n=1}^{N} s_n e^{\lambda_n} = 0, \tag{29}$$

where $\lambda_n = \rho_0 + \rho_1 + \ldots + \rho_M$ and hence $\{\lambda_1, \ldots, \lambda_N\}$ is conjugate complete by Lemma 3.31, and s_n are integer linear combinations of products of β_m's, and at least one s_n is nonzero.

We can rewrite (29), grouping the terms with the same coefficients and expanding it in the form

$$\kappa_0 E_0 + \kappa_1 E_1 + \ldots + \kappa_L E_L = 0, \tag{30}$$

where some E_i might equal some E_j (with $\kappa_i \neq \kappa_j$) but all $E_0, \ldots, E_L$ will be conjugate-complete simple exponential sums. What is important is that since at least one of the s_n's is not zero then at least one of $\kappa_0, \ldots, \kappa_L$ will be nonzero. Some κ_l's nontheless can be zero, and by omitting those terms and re-indexing we can assume that without loss of generality, all κ_l's are nonzero.

Now - the κ_l's are algebraic, as integer combinations of algebraic numbers. So our next step will be to do an analogous multiplication, this time by all conjugates of κ_l's

$$\prod_{\substack{\gamma_l \text{ is a conjugate of } \kappa_l \\ l=0,1,\ldots,L}} (\gamma_0 E_0 + \gamma_1 E_1 + \ldots + \gamma_L E_L) = 0. \tag{31}$$

After multiplication and factoring out equal coefficients, we arrive at

$$\eta_0 \mathcal{E}_0 + \eta_1 \mathcal{E}_1 + \ldots + \eta_K \mathcal{E}_K = 0, \tag{32}$$

where the η_k's are symmetric polynomials in the β_l's and their conjugates with integer coefficients, and the $\mathcal{E}_k$'s are products of the E_l's. Again looking at this product with regard to Lemma 3.29, we conclude that at least one η_k is nonzero. Also, since the η_k's are symmetric polynomials in the β_l's and their conjugates with integer coefficients, we have that all η_k's are rational numbers.

By multiplying (32) with the least common denominator of all the η_k's, without loss of generality, we may assume that all η_k's are nonzero integers. Since $\mathcal{E}_k$'s are finite products of the conjugate complete simple exponential sums E_l, by Corollary 3.36 we get that each $\mathcal{E}_k$ is a conjugate complete simple exponential sum. As in the special case - Theorem 3.9 - by regrouping and reindexing (32), we may again assume without loss of generality that all the exponents in $\mathcal{E}_k$ are conjugates of one another (ie are a complete collection of conjugates in the sense of Definition 3.6). The only thing that remains to be done is to reduce the equation (32) to the form where, say, $\mathcal{E}_0 = 1$.

Case (1). If we are lucky and one $\mathcal{E}_k$ is already equal to 1, we may directly apply Theorem 3.9.

Case (2). Now suppose that for all k, we have $\mathcal{E}_k \neq 1$ and let $\mathcal{E}_0 = e^{\nu_1} + e^{\nu_2} + \ldots + e^{\nu_J}$ and $\{\nu_1, \ldots, \nu_J\} \subset \overline{\mathbb{Q}} \setminus \{0\}$, with $\{\nu_1, \ldots, \nu_J\}$ a complete set of conjugates. Note that if one $\nu_j = 0$ then all must be equal to 0, since $\{\nu_1, \ldots, \nu_J\}$ is a complete collection of conjugates. Define $\mathcal{E}_0^{-1} = e^{-\nu_1} + e^{-\nu_2} + \ldots + e^{-\nu_J}$. Then obviously this is also a conjugate complete simple exponential sum, because $\{-\nu_1, \ldots, -\nu_J\}$ is a complete collection of conjugates. Hence by Corollary 3.36, $\mathcal{E}_0 \mathcal{E}_0^{-1}$ is a conjugate complete simple exponential sum.

$$\begin{aligned} \mathcal{E}_0 \mathcal{E}_0^{-1} &= \left(e^{\nu_1} + e^{\nu_2} + \ldots + e^{\nu_J}\right)\left(e^{-\nu_1} + e^{-\nu_2} + \ldots + e^{-\nu_J}\right) \\ &= e^0 + e^0 + \ldots + e^0 + \ldots = J + \mathcal{E}_0'', \end{aligned}$$

where $\mathcal{E}_0''$ is some conjugate complete simple exponential sum (because the exponents, by Lemma 3.33, form a complete set of conjugates and $e^0 = 1$ is a conjugate of only itself). Note also that in (32), for $k_1 \neq k_2$, each exponent appearing in $\mathcal{E}_{k_1}$ is different from each exponent of $\mathcal{E}_{k_2}$ (because the exponents in each $\mathcal{E}_k$ are complete collection of conjugates). This ensures that when we multiply (32) by $\mathcal{E}_0^{-1}$, i.e.

$$\eta_0 \mathcal{E}_0 \mathcal{E}_0^{-1} + \eta_1 \mathcal{E}_1 \mathcal{E}_0^{-1} + \ldots + \eta_K \mathcal{E}_K \mathcal{E}_0^{-1} = 0, \tag{33}$$

none of $\mathcal{E}_k'' = \mathcal{E}_0^{-1} \mathcal{E}_k$ will contain any e^0 terms. Also, we again have that each $\mathcal{E}_k''$ is a conjugate complete simple exponential sum. Then (33) can be rewritten as

$$J\eta_0 + \eta_0 \mathcal{E}_0'' + \eta_1 \mathcal{E}_1'' + \ldots + \eta_K \mathcal{E}_K'' = 0, \tag{34}$$

and finally as

$$\beta_0' + \beta_1' e^{\lambda_1} + \ldots + \beta_S' e^{\lambda_S} = 0, \tag{35}$$

where $\{\beta_0', \beta_1', \ldots, \beta_S'\} \subset \mathbb{Z} \setminus \{0\}$ and $\{\lambda_1, \ldots, \lambda_S\} \in [\mathbb{Q}]^S$ is a complete set of conjugates. Now we can apply Theorem 3.9 to reach the desired contradiction.

□

Having finished this proof, we give some of the more popular consequences of the Lindemann-Weierstraß Theorem.

3.38 Corollary (Hermite)**.** *If $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, then $e^\alpha \notin \overline{\mathbb{Q}}$.*

Proof. Suppose $e^\alpha \in \overline{\mathbb{Q}}$, then $e^\alpha = \beta$ for some $\beta \in \overline{\mathbb{Q}}$. Then $-\beta + e^\alpha = 0$, which contradicts the Lindemann-Weierstraß Theorem applied for $\{\alpha, 0\} \in [\overline{\mathbb{Q}}]^2$ and $\{1, -\beta\} \in \overline{\mathbb{Q}} \setminus \{0\}$. □

3.39 Note. An interesting direct proof of Hermite for real α is also given by Nesterenko in [23].

3.40 Corollary. *If $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, then $e^{i\alpha} \notin \overline{\mathbb{Q}}$.*

Proof. Note that $i\alpha$ is also algebraic, so by Corollary 3.38, $e^{i\alpha} \notin \overline{\mathbb{Q}}$. □

3.41 Corollary (Hermite-Lindemann Theorem)**.** *If $\{\alpha_0, \alpha_1, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}} \setminus \{0\}]^{M+1}$ and $\{\beta_0, \ldots, \beta_M\} \subset \overline{\mathbb{Q}} \setminus \{0\}$, then the number*

$$\sum_{m=0}^{M} \beta_m e^{\alpha_m}$$

is transcendental.

Proof. Suppose $\sum_{m=0}^{M} \beta_m e^{\alpha_m} = \gamma \in \overline{\mathbb{Q}}$. Define $\alpha_{M+1} = 0$ and $\beta_{M+1} = -\gamma$. Then we have that

$$\sum_{m=0}^{M+1} \beta_m e^{\alpha_m} = 0,$$

which contradicts the Lindemann-Weierstraß Theorem applied for $\{\alpha_0, \ldots \alpha_{M+1}\} \in [\overline{\mathbb{Q}}]^{M+2}$ and $\{\beta_0, \ldots, \beta_{M+1}\} \subset \overline{\mathbb{Q}} \setminus \{0\}$. □

3.42 Corollary. *If $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, then $\log \alpha$ is transcendental.*

Proof. Note $e^{\log \alpha} = \alpha \in \overline{\mathbb{Q}}$, so $\log \alpha$ can't be algebraic, since this would contradict Hermite's Theorem. □

3.43 Corollary. *If $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, then $\{\cos \alpha, \sin \alpha, \tan \alpha\} \cap \overline{\mathbb{Q}} = \emptyset$.*

Proof. Suppose $\cos \alpha = \beta \in \overline{\mathbb{Q}} \setminus \{0\}$. Now,

$$\beta = \cos \alpha = \frac{e^{i\alpha} + e^{-i\alpha}}{2},$$

so

$$-\beta e^0 + \frac{1}{2} e^{i\alpha} + \frac{1}{2} e^{-i\alpha} = 0,$$

which contradicts the Lindemann-Weierstraß Theorem applied for $\{-\beta, \frac{1}{2}, \frac{1}{2}\} \subset \overline{\mathbb{Q}} \setminus \{0\}$ and $\{0, i\alpha, -i\alpha\} \in [\overline{\mathbb{Q}}]^3$.

Similarly, we use the identity $\sin \alpha = \frac{e^{i\alpha} - e^{-i\alpha}}{2i}$ and assume $\sin \alpha = \beta \in \overline{\mathbb{Q}}$ to get a contradiction to Lindemann-Weierstraß for $\{0, i\alpha, -i\alpha\} \in [\overline{\mathbb{Q}}]^3$ and $\{\beta, \frac{i}{2}, \frac{-i}{2}\}$.

If

$$\tan \alpha = \frac{\sin \alpha}{\cos \alpha} = \frac{e^{i\alpha} - e^{-i\alpha}}{i(e^{i\alpha} + e^{-i\alpha})} = \beta \in \overline{\mathbb{Q}},$$

then

$$(i\beta - 1)e^{i\alpha} + (i\beta + 1)e^{-i\alpha} = 0.$$

Since $\alpha \neq 0$, $\{i\alpha, -i\alpha\} \in [\overline{\mathbb{Q}}]^2$, and $\{i\beta - 1, i\beta + 1\} \subset \overline{\mathbb{Q}} \setminus \{0\}$, and hence obtain a contradiction to the Lindemann-Weierstraß Theorem. □

More generally, using the idea that in order to prove $\sin\alpha, \cos\alpha, \tan\alpha$ were transcendental, we considered some polynomials in different powers of e^z, we can prove the following:

3.44 Theorem. *Let $P(z_1, \ldots, z_K)$ and $Q(z_1, \ldots, z_L)$ be two nonzero polynomials with integer coefficients. Let $\{\gamma_1, \ldots, \gamma_K\} \cup \{\eta_1, \ldots, \eta_L\} \subset \overline{\mathbb{Q}}$. Then the number*

$$\beta = \frac{P(e^{\gamma_1}, \ldots, e^{\gamma_K})}{Q(e^{\eta_1}, \ldots, e^{\eta_L})}$$

is either rational or transcendental.

3.45 Note. We provide a detailed proof that is only sketched in [6].

Proof. Assume that $\beta \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$. Then we have

$$\beta Q(e^{\eta_1}, \ldots, e^{\eta_L}) - P(e^{\gamma_1}, \ldots, e^{\gamma_K}) = 0. \tag{36}$$

Though some η_l's might equal some γ_k's, the common exponential terms in 36 cannot cancel out since β is irrational and Q and P are with integer coefficients. Let $M \in \mathbb{N}^+$ be such that both $\{\alpha_1, \ldots, \alpha_M\} \subseteq \{\gamma_1, \ldots, \gamma_K\} \cup \{\eta_1, \ldots, \eta_L\}$ are all different and M is the number of the nonzero coefficients in (36) after factoring the common exponential terms. Then (36) can be rewritten as:

$$\beta_1 e^{\alpha_1} + \ldots + \beta_M e^{\alpha_M} = 0, \tag{37}$$

where $\{\alpha_1, \ldots, \alpha_M\} \in [\overline{\mathbb{Q}}]^M$ and $\{\beta_1, \ldots, \beta_M\} \subseteq \overline{\mathbb{Q}} \setminus \{0\}$, hence contradicting the Lindemann-Weierstraß Theorem. □

In view of the above Theorem, and the proof of the Lindemann-Weierstraß Theorem which we provided, we can now see that the Lindemann-Weierstraß Theorem is equivalent to the following:

3.46 Theorem. *If $P(z_0, \ldots, z_M) = b_0 z_0 + \ldots + b_M z_M$ is a nonzero polynomial with $b_m \in \mathbb{Z}$ and $\{\alpha_0 \ldots, \alpha_M\} \in [\overline{\mathbb{Q}}]^{M+1}$, then $P(e^{\alpha_0}, \ldots, e^{\alpha_M}) \neq 0$.*

This leads us to the following theorem:

3.47 Theorem. *If $\{\alpha_0, \ldots, \alpha_M\} \subset \overline{\mathbb{Q}}$ are $\mathbb{Z}$-linearly independent, then $e^{\alpha_0}, \ldots, e^{\alpha_M}$ are algebraically independent.*

In [6], the converse is also given without proof:

3.48 Theorem. *Let $\{\alpha_0, \ldots, \alpha_M\} \subset \overline{\mathbb{Q}}$ and $e^{\alpha_0}, \ldots, e^{\alpha_M}$ be $\mathbb{Z}$-algebraically independent; then $\alpha_0, \ldots, \alpha_M$ are $\mathbb{Z}$-linearly independent.*

Proof. Suppose $\{\alpha_0, \ldots, \alpha_M\}$ are $\mathbb{Z}$-linearly independent and let $\{d_0, \ldots, d_m\} \subset \mathbb{Z} \setminus \{0\}$ be such that $d_0\alpha_0 + \ldots + d_M\alpha_M = 0$. Then

$$d_0\alpha_0 = -d_1\alpha_1 - \ldots - d_M\alpha_M,$$

so

$$e^{d_0\alpha_0} = e^{-d_1\alpha_1 - \ldots - d_M\alpha_M} = e^{-d_1\alpha_1} \ldots e^{-d_M\alpha_M},$$

hence

$$(e^{\alpha_0})^{d_0} - (e^{\alpha_1})^{-d_1} \ldots (e^{\alpha_M})^{-d_M} = 0. \tag{38}$$

Define the polynomial

$$P(z_0, \ldots, z_M) = z_0^{d_0} - z_1^{-d_1} \ldots z_M^{-d_M}.$$

Then (38) becomes

$$P(e^{\alpha_0}, e^{\alpha_1}, \ldots, e^{\alpha_M}) = 0, \tag{39}$$

a contradiction to the $\mathbb{Z}$-algebraic independence of $e^{\alpha_0}, \ldots, e^{\alpha_M}$. □

In fact, Theorem 3.47 can be restated in view of Schanuel's Conjecture as:

3.49 Theorem. *If $\alpha_0, \ldots, \alpha_M \in \overline{\mathbb{Q}}$ are $\overline{\mathbb{Q}}$-linearly independent numbers, then*

$$trdeg(\mathbb{Q}(\alpha_0, \ldots, \alpha_M, e^{\alpha_0}, \ldots, e^{\alpha_M})) = M + 1.$$

3.2 The Gelfond-Schneider Theorem

The Gel'fond-Schneider Theorem provides a solution to Hilbert's seventh problem: to prove that whenever $\alpha, \beta \in \overline{\mathbb{Q}}$ with $\alpha \neq 0, 1; \beta \notin \mathbb{Q}$, then α^β is transcendental. We note that $\alpha^\beta = \exp(\beta \log \alpha)$, $\log \alpha$ being any logarithm of α. In 1934, the Russian mathematician Alexandr Gel'fond [11] and the German mathematician Theodor Schneider [29] independently proved Hilbert's seventh problem.

3.50 Theorem (The Gel'fond-Schneider Theorem)**.** *If $\alpha, \beta \in \overline{\mathbb{Q}} \setminus \{0\}$, $\alpha \neq 1$, and β is not a real rational number, then any value of α^β is transcendental.*

This formulation can be found in [25].

3.51 Proposition ([27])**.** *The following are equivalent formulations of the Gelfond-Schneider Theorem:*

1. *If $\alpha, \beta \in \overline{\mathbb{Q}}$, $\alpha \neq 0$, and $\log \alpha \neq 0$, and β is irrational, then $\alpha^\beta = \exp(\beta \log \alpha)$ is transcendental.*
2. *If $\alpha, \beta \in \overline{\mathbb{Q}}$, $\alpha, \beta \neq 0$, and if $\log \alpha$, $\log \beta$ are linearly independent over $\mathbb{Q}$, then $\log \alpha$, $\log \beta$ are linearly independent over $\overline{\mathbb{Q}}$.*
3. *If $\beta, \lambda \in \mathbb{C}$, $\lambda \neq 0$, $\beta \notin \mathbb{Q}$, then one of the numbers e^λ, β, $e^{\beta\lambda}$ is transcendental.*

For more historical information and a comparison of the proofs of Gel'fond and Schneider, the interested reader is referred to [40], [38, Chapter 13.7], and [37].

3.3 Baker's Theorem

In 1966, Alan Baker extended the Gel'fond-Schneider Theorem ([2], [3]), who proved the more general result that:

3.52 Theorem (Baker's Theorem)**.** *Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}} \setminus \{0\}$. If $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over $\mathbb{Q}$, then $1, \log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over $\overline{\mathbb{Q}}$.*

3.4 The Six Exponentials Theorem

The Six Exponentials Theorem is a natural continuation of the Lindemann-Weierstraß–Gel'fond-Schneider–Baker arc, but does not follow from any of them.

A proof of a special case of the Six Exponentials Theorem is attributed to Siegel in a paper by L. Alaoglu and P. Erdős [1] in 1944. It states that if p_1^x, p_2^x and p_3^x are rational numbers for three distinct primes p_1, p_2, p_3, then x is an integer. Over a decade later, two independent proofs of the Six Exponentials Theorem were published by S. Lang [17, Chapter 2] and K. Ramachandra [26]. The Six Exponentials Theorem can also be deduced from a much more general result by Theodor Schneider [30].

3.53 Note. Information and references for this brief historical overview were taken from [38] and [39].

3.54 Theorem (Six Exponentials). *Let $\beta_1, \beta_2 \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$, and let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ also be $\mathbb{Q}$-linearly independent. Then at least one of the six numbers*

$$e^{\alpha_1\beta_1}, e^{\alpha_1\beta_2}, e^{\alpha_2\beta_1}, e^{\alpha_2\beta_2}, e^{\alpha_3\beta_1}, e^{\alpha_3\beta_2}$$

is transcendental (over $\mathbb{Q}$).

3.55 Remark. We note that the conclusion of the Theorem implies that the two functions $e^{\beta_1 x}, e^{\beta_2 x}$, which are $\mathbb{Q}$-algebraically independent, cannot simultaneously take algebraic values over any three distinct, $\mathbb{Q}$-linearly independent points $\alpha_1, \alpha_2, \alpha_3$. We also note that the method of proof used was first introduced by Schneider [40]. It uses an auxiliary function of the form

$$F(z) = P(e^{\beta_1 z}, e^{\beta_2 z})$$

for a specific polynomial P. Then, we assume that $F(z)$ has many zeros, and use the Maximum Modulus Principle to reach a contradiction (again by constructing an integer $\mathcal{N}$ which violates the Fundamental Principle of Transcendental Number Theory).

4 Consequences of Schanuel's Conjecture

4.1 A Plethora of Conjectures

There are some interesting conjectures, which follow quite easily from Schanuel's Conjecture. We will mention a couple of consequences which can be found in [27], filling in details of proofs and giving some more explanations.

4.1 Conjecture (Gel'fond). *If $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, and $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}} \setminus \{0\}$ are such that $\log \beta_1, \ldots, \log \beta_n$ are also linearly independent over $\mathbb{Q}$, then*

$$e^{\alpha_1}, \ldots, e^{\alpha_n}, \log \beta_1, \ldots, \log \beta_n$$

are $\overline{\mathbb{Q}}$-algebraically independent.

4.2 Proposition. *Schanuel's Conjecture (2.1) implies Gel'fond's Conjecture 4.1.*

Proof. We have

$$\begin{aligned}
&\operatorname{trdeg}_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}\,(e^{\alpha_1}, \ldots, e^{\alpha_n}, \log \beta_1, \ldots, \log \beta_n)) \\
&= \operatorname{trdeg}_{\mathbb{Q}}(\mathbb{Q}\,(e^{\alpha_1}, \ldots, e^{\alpha_n}, \log \beta_1, \ldots, \log \beta_n)) && \text{by Note 1.19} \\
&\leqslant 2n && \text{by Proposition 1.18.}
\end{aligned}$$

Also,

$$\begin{aligned}
&\operatorname{trdeg}_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}\,(e^{\alpha_1}, \ldots, e^{\alpha_n}, \log \beta_1, \ldots, \log \beta_n)) \\
&= \operatorname{trdeg}_{\mathbb{Q}}(\mathbb{Q}\,(e^{\alpha_1}, \ldots, e^{\alpha_n}, \log \beta_1, \ldots, \log \beta_n)) && \text{by Note 1.19} \\
&\geqslant \operatorname{trdeg}_{\mathbb{Q}}(\mathbb{Q}\,(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}, \log \beta_1, \ldots, \log \beta_n, \beta_1, \ldots, \beta_n)) \\
&\geqslant 2n && \text{by SC.}
\end{aligned}$$

Hence, $e^{\alpha_1}, \ldots, e^{\alpha_n}, \log \beta_1, \ldots, \log \beta_n$ are $\overline{\mathbb{Q}}$-algebraically independent. □

As a special case of Conjecture 4.1, we have:

4.3 Conjecture. *[Algebraic Independence of Logarithms [38]] Let $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}} \setminus \{0\}$ and suppose that $\log \beta_1, \ldots, \log \beta_n$ are $\mathbb{Q}$-linearly independent. Then $\log \beta_1, \ldots, \log \beta_n$ are $\overline{\mathbb{Q}}$-algebraically independent.*

We note that Baker's Theorem 3.52 is a weaker version of Conjecture 4.3.

4.4 Conjecture. *If $\alpha, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$, $\alpha \neq 0, 1$, and $1, \beta_1, \ldots, \beta_n$ are linearly independent over $\mathbb{Q}$, then $\log \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}$ are $\overline{\mathbb{Q}}$-algebraically independent.*

Proof Assuming SC. By assumption on $1, \beta_1, \ldots, \beta_n$, we have that $\log \alpha, \beta_1 \log \alpha, \ldots, \beta_n \log \alpha$ are linearly independent over $\mathbb{Q}$, hence, by Schanuel's Conjecture,

$$\operatorname{trdeg}_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}\left(\log \alpha, \beta_1 \log \alpha, \ldots, \beta_n \log \alpha, \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}\right)) \geqslant n + 1.$$

Since by assumption $\alpha, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$, then we must have that $\log \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}$ are $\mathbb{Q}$-algebraically independent, which in turn implies their algebraic independence over $\overline{\mathbb{Q}}$. □

In fact, even some special cases of Conjecture 4.4 are still open, for example Conjecture 2.2 from the beginning of this dissertation. When $n = 1$ we have:

4.5 Conjecture. *If $\alpha, \beta \in \overline{\mathbb{Q}}$, $\alpha \neq 0, 1$, and $\beta \notin \mathbb{Q}$, then $\log \alpha, \alpha^{\beta}$ are algebraically independent over $\overline{\mathbb{Q}}$.*

Lang and Ramachandra independently stated special cases of yet another conjecture which follows from Schanuel's Conjecture:

4.6 Conjecture (Lang and Ramachandra)**.** *If $\alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent, and β is a transcendental number, then*

$$\mathit{trdeg}_{\mathbb{Q}}(\mathbb{Q}\left(e^{\alpha_1}, \ldots, e^{\alpha_n}, e^{\alpha_1 \beta}, \ldots, e^{\alpha_n \beta}\right)) \geqslant n - 1.$$

Another interesting consequence is:

4.7 Conjecture. *The numbers*

$$e, e^{\pi}, e^{e}, e^{i}, \pi, \pi^{\pi}, \pi^{e}, \pi^{i}, 2^{\pi}, 2^{e}, 2^{i}, \log \pi, \log 2, \log 3, \log \log 2, (\log 2)^{\log 3}, 2^{\sqrt{2}}$$

are $\mathbb{Q}$-algebraically independent (and, in particular, they are transcendental).

Space constraints prevent us from providing a proof of the implication, but it can be found in [27, pg 326].

We now turn to a conjecture by Lang, for which we need a preliminary definition.

4.8 Definition. We define the field E by transfinite induction on the ordinals:

1. $E_0 = \overline{\mathbb{Q}}$,
2. $E_{n+1} = \overline{E_n\,(e^x : x \in E_n)}$,
3. $E = E_\omega = \bigcup_{n \leqslant \omega} E_n$

4.9 Note. For ordinals $\alpha > w$, $E_\alpha = E$. In particular, $E_{\omega+1} = \overline{E_\omega\,(e^x : x \in E_\omega)} = \overline{E\,(e^x : x \in E)} = E$.

4.10 Proposition. *Schanuel's Conjecture implies that $\pi \notin E$.*

4.11 Note. This Proposition is stated in [27], and is a corollary to a more general result proved in [8]. We use their ideas to give a direct proof of Proposition 4.10, making a couple of notes from a Set-Theoretic point of view.

Proof. By contradiction: suppose that $\pi \in E$. Then there is an $n \in \mathbb{N}$ such that $\pi \in E_n$.

By strong induction on n, we show that for all n, $\pi \notin E_n$.

For the base case, we note that $\pi \notin E_0 = \overline{\mathbb{Q}}$ by Corollary 2.4.

For the inductive hypothesis, suppose that (1) $\pi \in E_{n+1}$, that $\pi \notin E_m$ for all $m \leqslant n$, and that (2) for all $m < n$, we have $E_{m+1} = \overline{\mathbb{Q}(\exp(E_m))}$. Then $\pi \in E_{n+1} = \overline{E_n(e^x : x \in E_n)}$, so π is algebraic over $E_n(e^x : x \in E_n)$.

$$\begin{aligned}
&\pi \in E_{n+1} \\
&= \overline{E_n(e^x : x \in E_n)} && \text{by definition} \\
&= \overline{\overline{\mathbb{Q}(\exp(E_{n-1}))}(\exp(E_n))} && \text{by IH, part (2)} \\
&= \overline{\mathbb{Q}(\exp(E_{n-1}))(\exp(E_n))} && \text{by theory of extension fields} \\
&= \overline{\mathbb{Q}(\exp(E_{n-1}))} && \text{Since } E_{n-1} \subseteq E_n.
\end{aligned}$$

So $\pi \in \overline{\mathbb{Q}(\exp(E_{n-1}))}$, so π is algebraic over $\mathbb{Q}(\exp(E_{n-1}))$. We will now show that there is a finite $A_n \subseteq E_n$ such that π is algebraic over $\mathbb{Q}(\exp(A_n))$. Since $\pi \in E_{n+1} = \overline{\mathbb{Q}(\exp(E_{n-1}))}$, there is a polynomial $F \in \mathbb{Q}(\exp(E_{n-1}))[x]$, $F(x) = a_0 + \ldots a_m x^m$ such that $F(\pi) = 0$.

Now, $a_i = \alpha_1 e^{\beta_{i1}} + \ldots + \alpha_r e^{\beta_i r_i}$ for some $\{\beta_1, \ldots, \beta_r, \alpha_1, \ldots, \alpha_r\} \in E_n$, not necessarily nonzero or distinct. So, taking $A_n = \bigcup\{\beta_{i1}, \ldots, \beta_{ir_i} : i = 1, \ldots, m\}$ we get that π is algebraic over $\overline{\mathbb{Q}(A_n)}$.

By similar arguments, this time applied to the elements of $A_n \subseteq E_n$, one obtains a finite subset $A_{n-1} \subseteq E_n$ such that all elements of A_n are algebraic over $\mathbb{Q}(\exp(A_{n-1}))$, and since $\mathbb{N}$ is bounded below by 0, after finitely many (actually, n many) steps we reach a finite $A_0 \subset \mathbb{Q}$ such that A_1 is algebraic over $\mathbb{Q}(\exp(A_0))$.

Now we take $A = \cup_{k \leqslant n} A_k \subseteq \mathbb{Q}(\exp(A_n))$. By the theory of extension fields, we may take $B \subseteq A$ such that $\{e^b : b \in B\}$ is a transcendence basis of $\mathbb{Q}(\exp(A_n))$. Then $\{\pi\} \cup B$ are $\mathbb{Q}$-linearly independent (since $\pi \notin E_k, \forall k \leqslant n$ by inductive hypothesis, part (1), and also since the algebraic independence of B implies its linear independence), and so, since i is also algebraic, $\{i\pi\} \cup B$ are $\mathbb{Q}$-linearly independent.

So we may apply Schanuel's Conjecture, and, recalling that $e^{i\pi} = -1 \in \mathbb{Q}$, obtain

$$\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\{i\pi\} \cup B \cup \exp(B)) \geqslant |B| + 1.$$

On the other hand, since $B \subseteq A$ and $\exp(B)$ is a transcendence basis of $\mathbb{Q}(\exp(A))$, we have that

$$\begin{aligned}
\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\{i\pi\} \cup B \cup \exp(B)) &= \operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\{i\pi\} \cup B \cup \exp(A)) \\
&= \operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\exp(A)) \\
&= \operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\exp(B)) \\
&\leqslant |B|,
\end{aligned}$$

since $\{e^b : b \in B\}$ is a transcendence basis of $\mathbb{Q}(\exp(A_n))$.

Hence, we have reached the required contradiction. Hence $\pi \notin E_{n+1}$, which concludes the proof. □

4.12 Definition. We define the field L by

1. $L_0 = \overline{\mathbb{Q}}$,
2. $L_{n+1} = \overline{L_n(\log x : x \in \mathbb{E}_n)}$,
3. $L = L_\omega = \bigcup_{n<\omega} L_n$,

again noting that $L_{\omega+1} = L$.

4.13 Definition. Let $F \supset K$ be a field extension and $K \subseteq F_1, F_2 \subseteq F$ be two subextensions. We say they are *linearly disjoint over* K if and only if whenever $\{x_1, \ldots, x_n\} \subset F_1$ is linearly independent over K, then $\{x_1, \ldots, x_n\}$ is also linearly independent over F_2.

Now, in [8], one may find a proof of this very interesting Theorem, based on an exercise from Lang [17]:

4.14 Theorem (Lang's Exercise)**.** *Schanuel's Conjecture implies that the fields E and L are linearly disjoint over $\mathbb{Q}$.*

Due to space limitations, we will omit the proof, but provide some interesting corollaries, which can be found in [36].

4.15 Corollary. *Schanuel's Conjecture implies that:*

1. *$L \cap E = \overline{\mathbb{Q}}$;*
2. *$\pi \notin E$ (Proposition 4.10+Theorem 4.14) and $e \notin L$ (proof similar to that of Proposition 4.10);*

The following corollary to 4.14 is interesting in light of Conjectures 4.3 and 4.7:

4.16 Corollary. *Schanuel's Conjecture implies that:*

1. *$\pi, \log \pi, \log \log \pi, \ldots$ are algebraically independent over E;*
2. *$e, e^e, e^{e^e}, \ldots$ are algebraically independent over L;*

4.2 Chow's Interesting Result

We note that the Hermite-Lindemann Theorem (2.3) can be restated as:

4.17 Theorem. *The only solution to equation*

$$e^\alpha = \beta \tag{40}$$

in the algebraic numbers is $\alpha = 0, \beta = 1$.

We know that equation (40) has many solutions for $\alpha, \beta \in \mathbb{C}$. But can we do better in narrowing down the domain over which it still has solutions? A natural idea would be to take $\overline{\mathbb{Q}}$ and close it with respect to taking exp and log, which leads us to the following definition:

4.18 Definition ([9])**.** A subfield F of $\mathbb{C}$ is *closed under* exp *and* log if (1) $\exp(x) \in F$ for all $x \in F$ and (2) $\log(x) \in F$ for all nonzero $x \in F$, where log is the branch of the natural logarithm function such that $-\pi < \mathrm{I}m(\log x) \leqslant \pi$ for all x. The *field $\mathbb{E}$ of EL numbers* is the intersection of all subfields of $\mathbb{C}$ that are closed under exp and log.

Now, let us make the question a bit more specific: rather than considering pairs (α, β), we consider the special case when $\alpha = -\beta$, so now we ask whether the equation

$$\alpha + e^\alpha = 0 \tag{41}$$

has a real root in $\mathbb{E}$. In [9], Timothy Chow claims that the Conjecture we have just stated is still unsolved:

4.19 Conjecture (Chow)**.** *The real root R of $\alpha + e^{\alpha} = 0$ is not in $\mathbb{E}$.*

4.20 Notation. We denote by $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ a finite sequence of complex numbers.

4.21 Theorem. *Schanuel's Conjecture implies that the real root R of $\alpha + e^{\alpha} = 0$ is not in $\mathbb{E}$.*

4.22 Definition. A *tower* is a finite sequence $A = (a_1, \ldots, a_n)$ of nonzero complex numbers such that for all $1 \leqslant i \leqslant n$, there exists an $m_i \in \mathbb{N}^+$ such that $a_i^{m_i} \in \mathbb{Q}\left[a_1, e^{a_1}, \ldots, a_{i-1}, e^{a_{i-1}}\right]$ or $e^{a_i m_i} \in \mathbb{Q}\left[a_1, e^{a_1}, \ldots, a_{i-1}, e^{a_{i-1}}\right]$ (or both). A tower is called *reduced* if the set $\{a_i\}$ is linearly independent over $\mathbb{Q}$. If $\beta \in \mathbb{C}$, then *a tower for* β is a tower $(a_1, \ldots, a_n)$ such that $\beta \in \mathbb{Q}\left[a_1, e^{a_1}, \ldots, a_n, e^{a_n}\right]$

4.23 Note. We have reworked the proof of Theorem 4.21, providing our own proof for the assertion that there is a tower for all elements of $\mathbb{E}$ which uses an inductive construction of $\mathbb{E}$ mentioned by Chow (but not used afterwards), and completely restructured the rest of the proof, so as to make it more concise.

Proof. Assume Schanuel's Conjecture, and assume for a contradiction that $R \in \mathbb{E}$. We prove the Theorem in several stages.

Claim (1). There is a tower for R.

First, we will show that $\mathbb{E}$ can be inductively constructed from countably many sets $\mathbb{E}_n$, and then we will prove the more general claim that there is a tower for any element of $\mathbb{E}$, by induction on the 'least level' $\mathbb{E}_N$ at which the element appears.

We define the *sets* $\mathbb{E}_n$ as follows:

$$\begin{aligned}
\mathbb{E}_0 =& \{0\} \\
\mathbb{E}_{n+1} =& \mathbb{E}_n \cup \{z_1 * z_2 : z_1, z_2 \in \mathbb{E}_n,\ * \in \{+, -, .\}\} \\
&\cup \left\{ \frac{z_1}{z_2} : z_1, z_2 \in \mathbb{E}_n, z_2 \neq 0 \right\} \\
&\cup \{\log z : z \in \mathbb{E}_n \setminus \{0\}\} \\
&\cup \{e^z : z \in \mathbb{E}_n\}
\end{aligned}$$

So the elements of $\mathbb{E}_{n+1}$ are obtained from those of $\mathbb{E}_n$ by applying one field operation to $z_1, z_2 \in \mathbb{E}_n$, or by taking exp or log of an element of $\mathbb{E}_n$. Then $\mathbb{E} = \bigcup_{n \in \mathbb{N}} \mathbb{E}_n$.

Indeed, $\mathbb{E} \subseteq \bigcup_{n \in \mathbb{N}} \mathbb{E}_n$, since $\mathbb{E}$ is defined as the intersection of all subfields of $\mathbb{C}$ closed under exp and log and $\bigcup_{n \in \mathbb{N}} \mathbb{E}_n$ is obviously such a subfield.

Also, $\bigcup_{n \in \mathbb{N}} \mathbb{E}_n \subseteq \mathbb{E}$. For suppose that $\bigcup \mathbb{E}_n \setminus \mathbb{E} \neq \emptyset$. Then there exists an $N \in \mathbb{N}$ with $\mathbb{E}_N \setminus \mathbb{E} \neq \emptyset$. Since $\mathbb{N}$ is well-ordered, without loss of generality we can take N to be the least such. Now, let $z \in \mathbb{E}_n \setminus \mathbb{E}$ and note that by leastness of N, $z \notin E_{N-1}$. Then z was obtained either by a field operation on $\mathbb{E}_{N-1}$ or by taking exp or log of an elements of $\mathbb{E}_{n-1}$. Since $z \notin \mathbb{E}$ but $\mathbb{E}_{N-1} \subseteq \mathbb{E}$, the former would contradict $\mathbb{E}$ being a field, and the latter would contradict $\mathbb{E}$ being closed under exp and log. Hence $E \supseteq \bigcup \mathbb{E}_n$.

Note that by the well-ordering of $\mathbb{N}$, we have that for $z \in \mathbb{E}$, there is a least $N \in \mathbb{N}$ such that $z \in \mathbb{E}_N$. We use induction on this least N to construct a tower for $z \in \mathbb{E}$.

For the base case, if $N = 0$, $\mathbb{E}_0 = \{0\}$, so $z = 0 \in \mathbb{Q}$, and so we can take the 'null sequence'.

For the inductive step, suppose that for every $n \leqslant N$, we have a tower for all $k \in \mathbb{E}_n$. Consider $\mathbb{E}_{N+1}$ and let $z \in \mathbb{E}_{N+1} \setminus \mathbb{E}_N$.

Case. If z is obtained via a field operation applied to $z_1, z_2 \in \mathbb{E}_N$, then by inductive hypothesis, there exist towers $A = (a_1, \ldots, a_k)$, and $B = (b_1, \ldots, b_l)$ for z_1, z_2 respectively. Then we define the tower C for z by $C = (a_1, \ldots, a_k, b_1, \ldots, b_l)$. To check the tower condition is satisfied at the boundary between a_k and b_l, we note that since B is a tower, there is an $m_1 \in \mathbb{N}^+$ such that either $b_1^{m_1} \in \mathbb{Q}$ or $e^{b_1 m_1} \in \mathbb{Q}$, and moreover $\mathbb{Q} \subseteq \mathbb{Q}(a_1, e^{a_1}, \ldots, a_k, e^{a_k})$. So $z_1, z_2 \in \mathbb{Q}\left(a_1, e^{a_1}, \ldots, a_k, e^{a_k}, b_1, e^{b_1}, \ldots, b_l, e^{b_l}\right)$, and since z was obtained from z_1 and z_2 by a field operation, it is also in the field $\mathbb{Q}\left(a_1, e^{a_1}, \ldots, a_k, e^{a_k}, b_1, e^{b_1}, \ldots, b_l, e^{b_l}\right)$.

Case. If z is obtained from $\mathbb{E}_N$ by taking $\exp x$ for $x \in \mathbb{E}_N$, with $A = (a_1, \ldots, a_k)$ a tower for x, then the tower for z is $B = (a_1, \ldots, a_k, \log z)$. Indeed, $\log z = x \in \mathbb{Q}(a_1, e^{a_1}, \ldots, a_k, e^{a_k})$, and $z = e^{\log z} \in \mathbb{Q}\left(a_1, e^{a_1}, \ldots, a_k, \log z, e^{\log z}\right)$.

Case. If z is obtained from $\mathbb{E}_N$ by taking $\log x$ for some $x \in \mathbb{E}_N$, with $A = (a_1, \ldots, a_k)$ a tower for x, then the tower for z is $B = (a_1, \ldots, a_k, z)$, since $e^z = e^{\log x} = x \in \mathbb{Q}(a_1, e^{a_1}, \ldots, a_k, e^{a_k})$, and $z \in \mathbb{Q}(a_1, e^{a_1}, \ldots, a_k, e^{a_k}, z, e^z)$.

This concludes the inductive step of the proof.

Now, since $R \in \mathbb{E}$, our claim shows that there is a tower for R, say $A = (a_1, \ldots, a_n)$. In order to use Schanuel's Conjecture on the extension field $\mathbb{Q}(a_1, e^{a_1}, \ldots, a_k, e^{a_k})$, we need for the set $\{a_i\}$ to be linearly independent, i.e. we need to find a reduced tower for R. This motivates our next claim:

Claim (2). There is a reduced tower for R.

If $R \in \mathbb{Q}$, then as before, we may take the tower B to be the empty sequence.

If $R \in \mathbb{E} \backslash \mathbb{Q}$, then we suppose that every tower for R is not reduced, and take $B = (b_1, \ldots, b_n)$ to be the 'shortest' such (so $n = \min\{m \in \mathbb{N} : C = (c_1, \ldots, c_m)$ is a tower for $R\} \geqslant 1$, since $R \notin \mathbb{Q}$). We will construct a shorter tower for R, hence reaching a contradiction. We define

$$i = \min\{k : \{b_1, \ldots, b_k\} \text{ is } \mathbb{Q}\text{-linearly dependent}\}.$$

So there are rational numbers $\dfrac{p_j}{q_j}$ in lowest terms, such that

$$b_i = \sum_{j=1}^{i-1} \frac{p_j}{q_j} b_j. \tag{42}$$

We will now show that the sequence

$$B' = \left(\frac{b_1}{q_1}, \frac{b_2}{q_2}, \ldots, \frac{b_{i-1}}{q_{i-1}}, b_{i+1}, \ldots, b_n\right)$$

is a tower for R.

Claim (3). The sequence

$$\left(\frac{b_1}{q_1}, \frac{b_2}{q_2}, \ldots, \frac{b_{i-1}}{q_{i-1}}\right)$$

is a tower.

Note that the proper initial segment of a tower B is also a tower.

We first show that for all $j \leqslant i - 1$,

$$\mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_j, e^{b_j}\right) \subseteq \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_j}{q_j}, e^{\frac{b_j}{q_j}}\right). \tag{43}$$

Let $j \in \{1, \ldots, i-1\}$, $z \in \mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_j, e^{b_j}\right)$. Then z can be expressed as a function $f(x_1, \ldots, x_{2j})$ with rational coefficients, evaluated at the n-tuple $(b_1, e^{b_1}, \ldots, b_j, e^{b_j})$. Since

$b_k = \left(\frac{b_k}{q_k}\right) q_k$ and $e^{a_k} = e^{\left(\frac{a_k}{q_k}\right) q_k}$ for all $k \leqslant i-1$, z can also be expressed as a function with rational coefficients, evaluated at $\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_j}{q_j}, e^{\frac{b_j}{q_j}}$, so

$$z \in \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_j}{q_j}, e^{\frac{b_j}{q_j}}\right).$$

Hence, inclusion (43) holds.

Now, for $j \in \{1, \ldots, i-1\}$ we have two cases:

Case (1). There is an $m_j \in \mathbb{N}^+$ with $b_j^{m_j} \in \mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_{j-1}, e^{b_{j-1}}\right)$. Then

$$\left(\frac{b_j}{q_j}\right)^{m_j} \in \mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_{j-1}, e^{b_{j-1}}\right) \subseteq \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{j-1}}{q_{j-1}}, e^{\frac{b_{j-1}}{q_{j-1}}}\right).$$

Case (2). There is an $m_j \in \mathbb{N}^+$ with $e^{b_j m_j} \in \mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_{j-1}, e^{b_{j-1}}\right)$. Then

$$e^{\left(\frac{b_j}{q_j}\right)(q_j m_j)} = e^{b_j m_j} \in \mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_{j-1}, e^{b_{j-1}}\right) \subseteq \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{j-1}}{q_{j-1}}, e^{\frac{b_{j-1}}{q_{j-1}}}\right).$$

So we may take $m_j^{'} = m_j q_j$, so either

$$\left(\frac{b_j}{q_j}\right)^{m_j^{'}} \in \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{j-1}}{q_{j-1}}, e^{\frac{b_{j-1}}{q_{j-1}}}\right),$$

or

$$e^{\left(\frac{b_j}{q_j}\right) m_j^{'}} \in \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{j-1}}{q_{j-1}}, e^{\frac{b_{j-1}}{q_{j-1}}}\right),$$

hence verifying that $\left(\frac{b_1}{q_1}, \frac{b_2}{q_2}, \ldots, \frac{b_{i-1}}{q_{i-1}}\right)$ is a tower.

Now, we return to proving the claim that

$$B' = \left(\frac{b_1}{q_1}, \frac{b_2}{q_2}, \ldots, \frac{b_{i-1}}{q_{i-1}}, b_{i+1}, \ldots, b_n\right)$$

is a tower for R. We will do this by showing

$$\mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_i, e^{b_i}\right) \subseteq \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{i-1}}{q_{i-1}}, e^{\frac{b_{i-1}}{q_{i-1}}}\right).$$

By equation (42), we have that

$$b_i \in \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{i-1}}{q_{i-1}}, e^{\frac{b_{i-1}}{q_{i-1}}}\right), \tag{44}$$

so

$$e^{b_i} = e^{\sum_{j=1}^{i-1} \frac{p_j}{q_j} b_j} = \prod_{j=1}^{i-1} e^{\left(\frac{b_j}{q_j}\right) p_j}.$$

Thus e^{b_i} is a monomial in $e^{\frac{b_1}{q_1}}, \ldots, e^{\frac{b_{i-1}}{q_{i-1}}}$, so

$$e^{b_i} \in \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{i-1}}{q_{i-1}}, e^{\frac{b_{i-1}}{q_{i-1}}}\right). \tag{45}$$

Now note that by our third Claim,

$$\mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_{i-1}, e^{b_{i-1}}\right) \subseteq \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{i-1}}{q_{i-1}}, e^{\frac{b_{i-1}}{q_{i-1}}}\right),$$

so combining this with (44) and (45), gives us

$$\mathbb{Q}\left(b_1, e^{b_1}, \ldots, b_i, e^{b_i}\right) \subseteq \mathbb{Q}\left(\frac{b_1}{q_1}, e^{\frac{b_1}{q_1}}, \ldots, \frac{b_{i-1}}{q_{i-1}}, e^{\frac{b_{i-1}}{q_{i-1}}}\right).$$

Since the towers B and B' share the tail from $i+1$ onwards, we have that B' is indeed a tower for R. Moreover, it is of length $n-1 < n = \min\{m \in \mathbb{N} : C = (c_1, \ldots, c_n) \text{ is a tower for } R\}$, hence reaching the required contradiction.

Note that by Hermite, $e^R = -R$ implies that R cannot be algebraic, and hence is transcendental.

So, if $A = (a_1, \ldots, a_n)$ is a reduced tower for R, we have that the length of A is at least 1. Without loss of generality, we may assume that $R \notin \mathbb{Q}(a_1, e^{a_1}, \ldots, a_i, e^{a_i})$ for $i < n$ (for the well-ordering of $\mathbb{N}$ implies there is a least $N \in \mathbb{N}$ for which $(a_1, \ldots, a_N)$ is a tower for R).

Define $A' = (a_1, \ldots, a_n, R)$. Then $R \in \mathbb{Q}(a_1, e^{a_1}, \ldots, a_n, e^{a_n})$, and since e^R is the additive inverse of R by definition of R, we have $e^R \in \mathbb{Q}(a_1, e^{a_1}, \ldots, a_n, e^{a_n})$, as well.

Claim (4). If $A' = (a_1, \ldots, a_n)$ is a reduced tower, then exactly one of a_n and e^{a_n} is algebraic over $\mathbb{Q}(a_1, e^{a_1}, \ldots, a_{n-1}, e^{a_{n-1}})$.

By definition of a tower, we have that at least one of the number a_n and e^{a_n} is algebraic over $\mathbb{Q}(a_1, e^{a_1}, \ldots, a_{n-1}, e^{a_{n-1}})$, so $\operatorname{trdeg}(\mathbb{Q}(a_1, e^{a_1}, \ldots, a_n, e^{a_n})) \leqslant n$.

On the other hand, since the set $\{a_1, \ldots, a_n\}$ is linearly independent over $\mathbb{Q}$, Schanuel's Conjecture implies that the transcendence degree of $\mathbb{Q}(a_1, e^{a_1}, \ldots, a_n, e^{a_n})$ is at least n, so at most one of a_n and e^{a_n} is algebraic over $\mathbb{Q}(a_1, e^{a_1}, \ldots, a_n, e^{a_n})$.

Applying Claim 4 to the tower A', we get that A' cannot be a reduced tower; however, $A \subset A'$ is, so

$$R = \sum_{i=1}^{n} \frac{p_i a_i}{q_i}, \tag{46}$$

for some $p_i, q_i \in \mathbb{Z}$, $q_i \neq 0$. Since $R \notin \mathbb{Q}(a_1, e^{a_1}, \ldots, a_i, e^{a_i})$ for $i < n$, we have that $p_n \neq 0$.

So, substituting (46) into the equation for R gives us

$$\sum_{i=1}^{n} \frac{p_i a_i}{q_i} + \prod_{i=1}^{n} \left(e^{\frac{a_i}{q_i}}\right)^{p_i} \tag{47}$$

Defining $A'' = \left(\frac{a_1}{q_1}, \ldots, \frac{a_n}{q_n}\right)$ and using the same argument as before, we see that A'' is also a tower for R, and inherits its linear independence from A.

But $p_n \neq 0$, so (47) implies that $\frac{a_n}{q_n}$ is algebraic over $\mathbb{Q}(a_1, e^{a_1}, \ldots, a_{n-1}, e^{a_{n-1}})$ if and only if $e^{\frac{a_n}{q_n}}$ is. But we have seen that Schanuel's Conjecture and the definition of a tower show that exactly one of these must be algebraic, which is the desired contradiction.

Hence $R \notin \mathbb{E}$. □

In fact, Schanuel's Conjecture implies a stronger result, due to Lin [19]:

4.24 Theorem. *Schanuel's Conjecture implies that whenever $f(x, y) \in \overline{\mathbb{Q}}[x, y]$ is an irreducible polynomial and $f(\alpha, \exp(\alpha)) = 0$ for some $\alpha \in \mathbb{C} \setminus \{0\}$, then $\alpha \notin \mathbb{L}$, where $\mathbb{L}$ is the smallest algebraically closed subfields of $\mathbb{C}$ that is closed under* exp *and* log.

However, the proof is more involved than that of the elegant partial version we have shown.

4.3 More Consequences

A curious result is given by Sondow [31]:

4.25 Theorem. *Assuming Schanuel's Conjecture, let $z, w \in \mathbb{C} \setminus \{0, 1\}$. If both $z^w, w^z \in \overline{\mathbb{Q}}$, then z and w are either both rational or both transcendental.*

There is another very interesting consequence of Schanuel's Conjecture by Guiseppina Terzo [32], concerning algebraic relations among the elements of the exponential ring $(\mathbb{C}, e^x)$. Let us first give the formal definition, found in [32]:

4.26 Definition. An *exponential ring* is a pair (R, E) with R a commutative ring with 1 and $E : R \to \mathcal{U}(R)$ a morphism of the additive group of R into the multiplicative group of units of R satisfying $E(x + y) = E(x).E(y)$ for all $x, y \in R$, and $E(0) = 1$.

So, intuitively, E plays the role of the exponential function in the commutative ring R. For her result, Terzo uses a more general version of Schanuel's Conjecture, which holds for any exponential ring:

4.27 Conjecture (Schanuel's Condition)**.** *An exponential ring R satisfies Schanuel's Condition if R is a characteristic 0 domain and whenever $\alpha_1, \ldots, \alpha_n$ in R are linearly independent over $\mathbb{Q}$, the ring $\mathbb{Z}[\alpha_1, \ldots, \alpha_n, E(\alpha_1), \ldots, E(\alpha_n)]$ has transcendence degree at least n over $\mathbb{Q}$.*

We recall that:

4.28 Definition. [28] The *characteristic of a field K* is the smallest positive integer n with the property $nx = 0$ for all $x \in K$, and it is zero if no such n exists.

With these preliminaries in mind, Terzo's result states:

4.29 Theorem. *Assuming Schanuel's Conjecture, there are no further relations between π and i except the known ones, $e^{i\pi} = -1$ and $i^2 = -1$.*

5 Overview of Zilber's Result and Applications of Schanuel's Conjecture in Model Theory

> "It's always a pleasure to introduce ideas from model theory to people who do real mathematics." Professor Boris Zilber

In a paper published in 2005 [44], Boris Zilber provided a fascinating, novel approach to thinking about Schanuel's Conjecture: he used a model-theoretic construction to introduce a function called *pseudoexponentiation*, which is a map from the additive group of the underlying field to its multiplicative group, and behaves much like 'real' exponentiation. To be more precise, he showed that there is a sentence Φ in a certain infinitary language $\mathcal{L} = \{+, ., E, 0, 1\}$ about algebraically closed exponential fields such that Φ has a unique model of power κ for each uncountable cardinal κ.

For the exact Theorem, we need a preliminary definition:

5.1 Definition. Let $X \subseteq K$ be finite. We define a *dimension*

$$\partial(X) = \sup\{\text{trdeg}(Y \cup E(\text{span}(Y)) - \text{lindim}(Y) : X \subseteq Y \text{ is finite}\}$$

and a *closure operator*

$$\text{cl}(X) = \{a : \partial(X) = \partial(Xa)\}.$$

Thus, Zilber's Theorem may be stated as:

5.2 Theorem ([44])**.** *For all uncountable cardinals κ, there is a unique model of Φ of cardinality κ. If $(K, +, ., E) \models \Phi$, then every definable subset of K is countable or with countable complement. If $A \subseteq K$ is finite and $a, b \notin cl(A)$ there is an automorphism of K taking a to b.*

Moreover, if $(K, +, ., E) \models \Phi$, then $(K, +, ., E)$ satisfies the following five axioms (from [42]):

Axiom (EXP)**.** We have:

$$E(x_1 + x_2) = E(x_1).E(x_2)$$
$$\ker(E) = \pi\mathbb{Z}, \text{ some } \pi \in K.$$

Axiom (SCH)**.**

$$\text{trdeg}(X \cup E(X)) - \text{lindim}(X) \geqslant 0,$$

where $\text{lindim}(X)$ is the maximal size of a linearly independent subset (linear dimension).

Axiom (EC)**.** For any non-overdetermined irreducible system of polynomial equations

$$P(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0$$

there exists a generic solution satisfying

$$y_i = E(x_i) \ i = 1, \ldots, n.$$

Axiom (CC)**.** Analytic subsets of K^n of dimension 0 are countable.

Axiom (ACF_0)**.** Axioms for algebraically closed fields of characteristic 0.

Further, Zilber conjectured that:

5.3 Conjecture. *The field of complex numbers with exponentiation, $\mathbb{C}_{\exp}$, is isomorphic to the unique field with exponentiation K_E of cardinality $2^{\aleph_0}$.*

5.4 Note. We used material from [42], [22], and [15] for this overview.

Space limitations prevent us from surveying some more model-theoretic consequences of Schanuel's Conjecture. The interested reader is reader is refered to [21, Chapter 3.4],[43], and [33], and we state one interesting and one very important result, which answers a question by Tarski ([21]):

5.5 Theorem (interesting result)**.** *[16] There are at most countably many essential counterexamples to Schanuel's Conjecture.*

5.6 Theorem. *[20] Schanuel's Conjecture implies that the real field with exponentiation, $\mathbb{R}_{\exp}$, is decidable.*

6 Conclusion

We have seen that many central and interesting theorems and conjectures from a variety of areas follow from Schanuel's Conjecture. Transcendental Number Theory provides the natural setting for this conjecture, where natural, but also conjectural, generalisations, follow readily from Schanuel's. Model Theory not only gives unexpected applications of the Conjecture, in light of Tarski's question, but also provides the promise of a proof, or at least more grounds for faith in Schanuel's Conjecture, via Zilber's pseudoexponentiation.

References

[1] L. Alaoglu and P. Erdös. On highly composite and similar numbers. *Trans. Amer. Math. Soc.*, 56:448–469, 1944.

[2] Alan Baker. Linear forms in the logarithms of algebraic numbers. I. *Mathematika. A Journal of Pure and Applied Mathematics*, 13:204–216, 1966.

[3] Alan Baker. Linear forms in the logarithms of algebraic numbers. II. III. *Mathematika. A Journal of Pure and Applied Mathematics*, 14:102–107,220–228, 1967.

[4] Alan Baker. *Transcendental Number Theory.* Cambridge University Press, 1990.

[5] Frits Beukers, Jean-Paul Bezivin, and Philippe Robba. An Alternative Proof of the Lindemann-Weierstraß Theorem. *The American Mathematical Monthly*, 97(3):193–197, 1990.

[6] Edward Burger and Robert Tubbs. *Making Transcendence Transparent.* Springer Science Business Media Inc, 2004.

[7] Lee Butler. Transcendence and irrationality proofs. `http://www.maths.bris.ac.uk/~malab/PDFs/MA469.pdf`. Fourth year project.

[8] Chuangxun Cheng, Brian Dietel, Mathilde Herblot, Jingjing Huang, Holly Krieger, Diego Marques, Jonathan Mason, Martin Mereb, and S Robert Wilson. Some consequences of schanuel's conjecture. *Arizona Winter School 2008*, 2008.

[9] Timothy Chow. What is a Closed-Form Number? *The American Mathematical Monthly*, 106(5):440–448, 1999.

[10] Heinrich Dörrie. *100 Great Problems of Elementary Mathematics.* Dover Publications Inc, 1965.

[11] Aleksandr Gel'fond. Sur le septiéme probléme de D. Hilbert. *Izv. Akad. Nauk SSSR*, 7:623–630, 1934.

[12] Derek Goldrei. *Classic Set Theory For Guided Independent Study.* Chapman & Hall, 1st edition, 1996.

[13] Charles Hermite. Sur la fonction exponentielle. *Compte Rendu Academie Scientifique*, 77:18–24, 1873.

[14] Jonathan Kirby. Variants of Schanuel's Conjecture. `http://www.uea.ac.uk/~ccf09tku/pdf/SCvariants.pdf`, Sept 2007. Expository article.

[15] Jonathan Kirby. Complex Exponentiation and Zilber's Pseudo-exponentiation. `http://at.yorku.ca/cgi-bin/bbqa?forum=ask_a_topologist;task=show_msg;msg=1977`, Apr 2009. Online Resource.

[16] Jonathan Kirby. Exponential algebraicity in exponential fields. *Bulletin of the London Mathematical Society*, 42(5):879–890, 2010.

[17] Serge Lang. *Introduction to Transcendental numbers.* Addison-Wesley Publishing Co, 1966.

[18] Serge Lang. *Algebra.* Graduate Texts in Mathematics. Springer, 3d edition, 2002.

[19] F.-C. Lin. Schanuel's conjecture implies Ritt's conjecture. *Chinese J. Math*, pages 41–50, 1983.

[20] Angus Macintyre and Alex Wilkie. *On the decidability of the real exponential field.* Number CLSI. 1995.

[21] David Marker. *Model Theory: an Introduction.* Springer-Verlag, New York, 2002.

[22] David Marker. A remark on Zilber's pseudoexponentiation. *Journal of Symbolic Logic*, 71:791–798, 2006.

[23] Yurii Nesterenko. On the number π and Lindemann's theorem. *Commentationes Mathematicae Universitatis Carolinae*, 20(2):335–343, 1979.

[24] Yurii Nesterenko. Modular functions and transcendence questions. *Mat. Sb*, 187:65–96, 1996.

[25] Ivan Niven. *The Carus Mathematical Monographs.* The Mathematical Association of America, second edition, 1956.

[26] Kanakanahalli Ramachandra. *Contributions to the theory of transcendental numbers. I, II.* Acta Arith., 1967/1968.

[27] Paulo Ribenboim. *My Numbers, My Friends: Popular Lectures on Number Theory.* Springer-Verlag New York, Inc, 2000.

[28] H. E. Rose. *A Course in Number Theory.* Oxford Science Publications. Oxford University Press, 1994.

[29] Theodor Schneider. Transzendenzuntersuchungen periodischer Funktionen. I. II. *J. Reine Angew. Math.*, 172:65–69,70–74, 1934.

[30] Theodor Schneider. Ein satz über ganzwertige funktionen als prinzip für transzendenzbeweise. *Math. Ann.*, 121:131–140, 1949.

[31] Jonathan Sondow and Diego Marques. Schanuel's Conjecture and algebraic powers z^w and w^z with z and w transcendental. *East-West Journal of Mathematics*, 12(1):75–84, 2010.

[32] Guiseppina Terzo. Some consequences of Schanuel's Conjecture in exponential rings. *Communications in Algebra*, 36:1171–1189, 2008.

[33] L. van den Dries, Angus Macintyre, and David Marker. On the elementary theory of restricted analytic functions with exponentiation. *Annals of Math.*, 140:183–205, 1994.

[34] Carl Louis Ferdinand von Lindemann. Über die Ludolph'sche Zahl. *Sitzungsberichte der Akademie der Wiss. Berlin*, 2:679–682, 1882.

[35] Michael Waldschmidt. Schanuel's Conjecture and Criteria for Algebraic Independence. `http://www.math.jussieu.fr/~miw/articles/pdf/SchanuelConjecture2009.pdf`. Online Beamer Presentation.

[36] Michael Waldschmidt. Some consequences of Schanuel's conjecture. `http://www.math.jussieu.fr/~miw/articles/pdf/AWSProject2.pdf`. Online Beamer Presentation.

[37] Michael Waldschmidt. Fonctions auxiliaires et fonctionnelles analytiques. I, II,. *J. Analyse Math.*, 56:231–254,255–279, 1991.

[38] Michael Waldschmidt. *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables.* Grundlehren der Mathematischens Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag Berlin, 2000.

[39] Michael Waldschmidt. Surveys in number theory. In Krishnaswami Alladi, editor, *Developments in Mathematics*. Springer, 1st edition, 2008.

[40] Michael Waldschmidt. Auxiliary functions in transcendental number theory. *The Ramanujan journal*, 20(3):341–373, 2009.

[41] K. Weierstraß. Zu Lindemann's Abhandlung "Über die Ludolph'sche Zahl". *Sitzungsber. Preuß. Akad. Wiss. zu Berlin*, 2:1067–1085, 1885.

[42] Boris Zilber. On transcendental number theory, classical analytic functions and Diophantine geometry. `http://www.phil.uu.nl/~iemhoff/Beauty/ZilberDay.pdf`. Online resource.

[43] Boris Zilber. Exponential sums equations and the Schanuel conjecture. *Journal of the London Mathematical Society*, 65:27–44, 2002.

[44] Boris Zilber. Pseudo-exponentiation on algebraically closed fields of characteristic zero. *Annals of Pure and Applied Logic*, 132(1):67–95, 2005.