Monograph on Number Theory
Indian National Science Academy
R.P. Bambah, V.C. Dumir and R.J. Hans Gill eds.

Algebraic Independence of Transcendental Numbers: A Survey

by

Michel WALDSCHMIDT

Abstract.
A survey on algebraic independence of transcendental numbers by Gel'fond's method was published by the author in 1984 [84 W1]. Here we cover the recent period 1984/1997.

Introduction

Important progress concerning algebraic independence of transcendental numbers has been achieved recently. Our goal is to introduce some of the most important ones. So many new results have been produced that we need to make a choice: here we wish to concentrate our survey on the description of new results which are related with Gel'fond's method. However we shall also include other topics (like Nesterenko's results on modular functions). Moreover our list of references will cover a broader scope.

Here is a short list of some of the many topics which are not covered here.

- Works involving the method of Siegel and Shidlovskiĭ, including values of hypergeometric functions. One main reference on this topic is Shidlovskiĭ's book [87 Shi2] and [89 Shi2]. Among many contributions to this subject, we mention those of Shidlovskiĭ himself [87 Shi1], [89 Shi1], [89 Shi3], [91 Shi1], [91 Shi2], as well as his work with Yu.V. Nesterenko [96 NS]. Several papers have been produced by other members of Shidlovskiĭ's school, including Yu.V. Nesterenko [88 Ne], V. Kh. Salikhov [84 Sal], [89 Sal], [90 Sal1], [90 Sal2], V. A. Kulagin [87 K], [91 K], [92 K], [96 K], N.I. Lossov [89 Lo], M.A. Cherepnev [90 Chr], [91 Chr], [94 Chr], [95 Chr], A.I. Zhukov [91 Zh] and V.A. Gorelov [92 Go]. Further references are [84 BV], [85 Br], [86 Br], [88 Beu] and [88 BeBrH]. Most of these articles are devoted to the study of algebraic independence of the values of solutions of differential equations, applying Siegel's or Shidlovskiĭ's main theorems.

- The method of Bézivin-Robba [89 BR], [90 BBR], which produces a new proof of the Lindemann-Weierstraß Theorem. We refer to Y. André's papers [96 An] and [98 An2], which explain connections with E-functions as well as with G-functions.
- *Mahler's method.* An excellent reference on this subject is Kumiko Nishioka's Lecture Notes [96 Ni1] where many further references are provided. See also [86 Ni1], [86 Ni2], [86 Ni3], [87 Ni], [88 Bec], [89 BN], [89 Ni], [90 Ni], [90 NN], [90 Wa], [91 Am], [91 Bec], [91 Ni], [92 Bec], [94 Ni], [94 Tö1], [95 Tö1], [95 Tö2], [96 Ni2], [96 Ni3], [96 Ta], [97 Ni] and [97 To].
- Liouville's argument yields not only transcendental numbers, but also algebraically independent numbers. This way of constructing algebraically independent numbers is related with results of transcendence or algebraic independence on values of gap series. Many authors have studied this question (see a survey in [90 W1]), including Zhu Yao Chen [84 Z], [85 Z2], [85 Z3], [87 Z], [88 Z], [89 WZ], [91 Z1], [91 Z2], as well as W.W. Adams [85 Ad], M. Amou [85 Am], [91 Am], P. Bundschuh [88 Bu], [90 Bu], R. Müller [93 Mü] and T. Töpfer [94 Tö2].
- *Transcendence and algebraic independence in finite characteristic.* The recent survey by W.D. Brownawell [98 Br] gives a good description of this rich theory, including the important achievements by Jing Yu [92 Y], [97 Y] as well as the works of A. Thiery [92 Th], W.D. Brownawell [93 Br], [94 BBT], [96 Br], R. Tubbs [96 Tu] and L. Denis [93 Den1], [93 Den2], [95 Den1], [95 Den2], [96 Den], [97 Den]. We also quote the work [93 Mü] by R. Müller which involves non archimedean valued fields.
  Also related to this topic is the paper [88 AMP] by J-P. Allouche, M. Mendès-France and A.J. van der Poorten, dealing with the algebraic independence over $F(X)$ of powers $f^{\lambda_1}, \ldots, f^{\lambda_s}$, where f is a formal power series, with coefficients in a finite field F, which is algebraic over $F(X)$.
- Metric theory and classifications of transcendental numbers.
- Lower bounds for linear forms in logarithms of algebraic numbers.

In this survey we first state a few conjectures (§1). Next we describe the methods of transcendence and algebraic independence (§2); some proofs of algebraic independence results involve a transcendence criterion, other ones rest on an effective version of Hilbert's Nullstellensatz; a more recent approach is via simultaneous Diophantine approximation Finally we state some of the most important recent progress on this topic, starting with Gel'fond's method (§3) considering results of algebraic independence related to the modular functions (§4) and finishing with Philippon's Diophantine rings (§5).

We would like to point out two important directions related with Gel'fond's method of algebraic independence:

- *Commutative algebraic groups*: the currently available tools and methods are well adapted to this geometrical setting, and a rather strong set of general results are available (even if we are far from being able to establish the main conjectures). A survey of this topic is [96 Ca].
- *Diophantine approximation and algebraic independence.* The connection between these two topics opens the way to a promising field of research. We discuss some of these new advances below (§2.4); a good starting point to get acquainted with this subject is [97 RW2].

1. Conjectures

In this section we collect various conjectures of algebraic independence. We start with Schanuel's one (see [84 W1] for references):

Conjecture 1.1. (Schanuel). *Let $x_1, \dots, x_n$ be $\mathbb{Q}$-linearly independent complex numbers. Then the transcendence degree over $\mathbb{Q}$ of the field*

$$\mathbb{Q}(x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n})$$

is at least n.

The following problem of A.O. Gel'fond and Th. Schneider (again, see [84 W1]) is a special case of Conjecture 1.1:

Conjecture 1.2. (Gel'fond-Schneider) *Let α be a non zero complex algebraic number, $\log \alpha$ a non zero logarithm of α and β an algebraic number of degree $d \geq 2$. For $z \in \mathbb{C}$, define $\alpha^z := \exp(z \log \alpha)$. Then the $d-1$ numbers*

$$\alpha^{\beta}, \alpha^{\beta^2}, \dots, \alpha^{\beta^{d-1}}$$

are algebraically independent.

It is equivalent to say that *for algebraic numbers $\beta_1, \dots, \beta_m$ which are pairwise distinct modulo $\mathbb{Z}$ [1], the numbers*

$$\alpha^{\beta_1}, , \dots, \alpha^{\beta_m}$$

are linearly independent over $\mathbb{Q}$ (or over $\overline{\mathbb{Q}}$, as you wish). However partial results are known on the question of algebraic independence, but almost nothing is known on the question of linear independence!

In 1949, A.O. Gel'fond solved Conjecture 1.2 in the case $d = 3$. More generally, he proved that for $d \geq 3$, two at least of the $d-1$ numbers in Conjecture 1.2 are algebraically independent. Such a result, which shows that some field has transcendence degree ≥ 2 over $\mathbb{Q}$, is a statement of "small transcendence degree". Showing that the transcendence degree tends to infinity with d (as achieved first by G.V. Chudnovsky) is proving a result of "large transcendence degree". Working with the exponential function, A.O. Gel'fond introduced two sets of $\mathbb{Q}$-linearly independent numbers, $(x_1, \dots, x_d)$ and $(y_1, \dots, y_\ell)$, and proved results of small transcendence degree involving the $d\ell$ values $e^{x_i y_j}$ $(1 \leq i \leq d,\ 1 \leq j \leq \ell)$.

Available methods of algebraic independence on such values of the exponential function which yield "large transcendence degrees" all require a so-called "technical hypothesis", namely a measure of linear independence for the tuple $(x_1, \dots, x_d)$ as well as for the tuple $(y_1, \dots, y_\ell)$.

Definition. We shall say that a set $\{x_1, \dots, x_n\}$ of $\mathbb{Q}$-linearly independent complex numbers *satisfies a measure of linear independence* if, for any $\epsilon > 0$, there exists a positive number H_0 such that, for any $H \geq H_0$ and n-tuple $(h_1, \dots, h_n)$ of rational integers satisfying $0 < \max\{|h_1|, \dots, |h_n|\} \leq H$, the inequality

$$|h_1 x_1 + \cdots + h_n x_n| \geq \exp\{-H^{\epsilon}\}$$

holds.

As a matter of fact, in the original papers, the actual results which we are going to discuss sometimes involve weaker assumptions (see [98 FN] for a more careful discussion). But we shall use this definition for convenience and simplicity.

Schanuel's Conjecture suggests that such a technical hypothesis should not be necessary, and it is a challenge to remove it (see [92 Del], [93 Del], [96 Del1] and [96 Del2]). Unfortunately, so far, only results of small transcendence degree are free of such an assumption.

---

[1] This means $\beta_i - \beta_j \notin \mathbb{Z}$ for $i \neq j$.

By the way, we take this opportunity to point out that the generalization of Schanuel's Conjecture which is suggested p. 566 of [84 W1] is too optimistic: it does not hold without a technical hypothesis, as shown by the following result of A. Bijlsma([2])

Lemma 1.3. (Bijlsma) *For any fixed natural number κ, there exist irrational numbers $a, b \in (0,1)$ such that for infinitely many triples (α, β, γ) of rational numbers*

$$\max\{|a-\alpha|, |b-\beta|, |a^b-\gamma|\} < \exp\bigl(-(\log H)^\kappa\bigr),$$

where H denotes the maximum of the heights of α, β and γ.

Recall that the *usual height* of a polynomial P with rational (and more generally complex) coefficients is the maximum of the absolute values of its coefficients, and the *(usual) height* of an algebraic number is the usual height of its minimal polynomial over $\mathbb{Z}$.

In place of the generalization of Schanuel's Conjecture suggested in [84 W1] section IV.2, we now propose the following statement, whose assumptions include a technical hypothesis:

Conjecture 1.4. *Let $x_1, \dots, x_n$ be $\mathbb{Q}$-linearly independent complex numbers which satisfy a measure of linear independence. Let d be a positive integer. Then there exists a positive number $C = C(x_1, \dots, x_n, d)$ with the following property: for any integer $H \geq 2$ and any $n+1$ tuple $P_1, \dots, P_{n+1}$ of polynomials in $\mathbb{Z}[X_1, \dots, X_n, Y_1, \dots, Y_n]$ with degrees $\leq d$ and usual heights $\leq H$, which generate an ideal of $\mathbb{Q}[X_1, \dots, X_n, Y_1, \dots, Y_n]$ of rank ([3]) $n+1$, we have*

$$\sum_{j=1}^{n+1} \bigl|P_j(x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n})\bigr| \geq H^{-C}.$$

One of the most important special cases of Schanuel's Conjecture deals with the set

$$\mathcal{L} = \bigl\{\ell \in \mathbb{C}\,;\, e^\ell \in \overline{\mathbb{Q}}^\times\bigr\}.$$

of logarithms of algebraic numbers:

Conjecture 1.5. (Conjecture on algebraic independence of logarithms of algebraic numbers) *If $\ell_1, \dots, \ell_n$ are $\mathbb{Q}$-linearly independent elements of $\mathcal{L}$, then they are algebraically independent.*

A formal analog of Conjecture 1.5, which answers a question of Y. Hellegouarch, has been established by D.L. McQuillan [85 Mc]:

Let k be a field of zero characteristic, $P_1, , P_2, \dots$ non constant polynomials in $k[x]$ which are pairwise relatively prime and satisfy $P_i(0) = 1$. Define, for $i \geq 1$,

$$\mathrm{Log} P_i = -\sum_{n=1}^{\infty} \frac{1}{n}\bigl(1 - P(x)\bigr)^n \in k((x)).$$

Then $\mathrm{Log} P_1, \mathrm{Log} P_2, \dots$ are algebraically independent over $k(x)$.

Let us come back to the classical case. From Conjecture 1.4 one deduces the following quantitative version of Conjecture 1.5: *Let $n \geq 2$ and $d \geq 1$ be positive integers and $a_1, \dots, a_n$ be multiplicatively*

([2]) Bijlsma, Alex – On the simultaneous approximation of a,b and a^b. Compositio Math. **35** (1977), no. 1, 99–111.

([3]) The rank of a prime ideal $\mathfrak{P} \subset \mathbb{Q}[T_1, \dots, T_m]$ is the largest integer $r \geq 0$ such that there exists an increasing chain of prime ideals $(0) = \mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_r = \mathfrak{P}$.

The rank of an ideal $\mathfrak{I} \subset \mathbb{Q}[T_1, \dots, T_m]$ is the minimum rank of a prime ideal containing $\mathfrak{I}$.

independent positive integers, i.e. positive elements in $\mathbb{Z}$ *such that the only relation* $a_1^{b_1} \cdots a_n^{b_n} = 1$ *with* $(b_1, \ldots, b_n) \in \mathbb{Z}$ *arises from the trivial case* $b_1 = \cdots = b_n = 0$. *Then there exists a constant* $C > 0$, *depending on* n, $a_1, \ldots, a_n$ *and also on* d, *such that, for any integer* $H \geq 2$ *and any non zero polynomial* P *in* $\mathbb{Z}[X_1, \ldots, X_n]$ *of degree* $\leq d$ *and height* $\leq H$,

$$|P(\log a_1, \ldots, \log a_n)| \geq H^{-C}.$$

Only the case of an homogeneous linear form $P = b_1 X_1 + \cdots + b_n X_n$ is known (Theorem of Baker-Fel'dman).

The work of D. Roy [92 R] yields a new approach to Conjecture 1.5, involving matrices whose coefficients are linear combinations, with algebraic coefficients, of elements of $\mathcal{L}$. For such a matrix M, say of size $d \times \ell$, he defines the *structural rank* $r_{\mathrm{str}}(M)$ of M as the rank ([4]) of the matrix $\widetilde{M}$ obtained from M by replacing with indeterminates a basis of the vector space over $\overline{\mathbb{Q}}$ spanned by the coefficients of M: if

$$M = M_0 + M_1 \ell_1 + \cdots + M_k \ell_k,$$

where $1, \ell_1, \ldots, \ell_k$ are $\overline{\mathbb{Q}}$-linearly independent, $\ell_j \in \mathcal{L}$ $(1 \leq j \leq k)$ and $M_j \in \mathrm{Mat}_{d \times \ell}(\overline{\mathbb{Q}})$ $(0 \leq j \leq k)$, then

$$\widetilde{M} = M_0 + M_1 X_1 + \cdots + M_k X_k \in \mathrm{Mat}_{d \times \ell}\big(\overline{\mathbb{Q}}(X_1, \ldots, X_k)\big).$$

It is neither surprising nor difficult to check that if Conjecture 1.5 holds, then the rank of M is equal to $r_{\mathrm{str}}(M)$. What is remarkable is the converse: *if the rank of* M *is always equal to* $r_{\mathrm{str}}(M)$, *then Conjecture 1.5 is true*.

In [95 R], D. Roy studies the set of points, whose coordinates are logarithms of algebraic numbers, which belong to a given algebraic variety. This work may be viewed as a first step towards the conjecture on algebraic independence of logarithms, since D. Roy remarks in [95 R] that Conjecture 1.5 is also equivalent to the following statement: *For each positive integer* n *and each algebraic subvariety* V *of* $\mathbb{C}^n$ *defined over* $\overline{\mathbb{Q}}$, *the set* $V \cap \mathcal{L}^n$ *is contained in the union of all vector subspaces of* $\mathbb{C}^n$ *defined over* $\mathbb{Q}$ *and contained in* V.

Further related conjectures of algebraic independence dealing with commutative algebraic groups are discussed in [96 W].

Conjectural extensions of Lindemann-Weierstraß Theorem to algebraic groups are considered in [87 P].

A conjectural description of the ideal of relations of algebraic dependence between periods of algebraic varieties which are defined over the field of algebraic numbers has been proposed by A. Grothendieck in 1966 and made more precise by S. Lang the same year. A joint generalization of Grothendieck's and Schanuel's Conjectures is suggested by Y. André [98 An1], who also proposes a transcendence conjecture on uniformization of Shimura's varieties, and discusses a non abelian variant of Grothendieck's Conjecture (see [97 Pr]), due to C. Simpson [90 Si], concerning the Riemann-Hilbert correspondence. Moreover in [98 An1] one can find comments on links between these conjectures and several topics, especially the Conjectures of Rohrlich and Lang on the algebraic dependence relations between values of the Gamma function, the results of Nesterenko on the modular functions (see §4 below), and the results of P. Cohen, H. Shiga and J. Wolfart, who extend in higher dimension Schneider's Theorem on the modular invariant j.

Notice that the conjectures in [86 W] are much less ambitious (and therefore should be easier to reach) than the general ones of Y. André in [98 An1]: they are more closely connected with currently available methods.

([4]) The rank of a matrix is the rank over the field generated by its entries.

A conjecture in the "folklore" is that the zeroes of the Riemann zeta function (say their imaginary parts, assuming it > 0) are algebraically independent. As suggested by J-P. Serre, one might be tempted to consider also

- The eigenvalues of the zeroes of the hyperbolic Laplacian in the upper half plane modulo $\mathrm{SL}_2(\mathbb{Z})$ (i.e. to study the algebraic independence of the zeroes of Selberg zeta function).
- The eigenvalues of the Hecke operators acting on the corresponding eigenfunctions (Maass forms).

2. Methods

2.1. Transcendence and Algebraic Independence

Given functions $f_1, \ldots, f_d$ and points $u_1, \ldots, u_\ell$, a central problem is to give, under suitable assumptions, a lower bound for the transcendence degree of the field generated over $\mathbb{Q}$ by the $d\ell$ numbers $f_i(u_j)$ $(1 \le i \le d,\ 1 \le j \le \ell)$. Here is an example with $d = 2$, $\ell = 1$ and $f_1(z) = z$: consider a given function f and an algebraic number α such that $f(\alpha)$ is also algebraic; one wishes to deduce that α belongs to a restricted set. If $f(z) = e^z$, the restricted set is just $\{0\}$; if $f(z) = e^{i\pi z}$, the restricted set is $\mathbb{Q}$.

In general, one deals with a finite set of numbers $\{\theta_1, \ldots, \theta_n\}$. In the last example one would take $n = 2$, $\theta_1 = \alpha$, $\theta_2 = f(\alpha)$

The basic methods of transcendence usually involve the construction of some number γ in the field $K = \mathbb{Q}(\theta_1, \ldots, \theta_n)$. This number γ typically is either the value of an auxiliary function, or the determinant of an interpolation matrix.

To start with, assume that all numbers $\theta_1, \ldots, \theta_n$ are algebraic. Therefore the number γ also is algebraic. Three main steps in the proof are:

- *Zero estimate*([5]): This number γ does not vanish.
- *Arithmetic estimate:* Lower bound for $|\gamma|$.
- *Analytic estimate:* Upper bound for $|\gamma|$.

We are interested here in the lower bound, which is a Liouville type argument: the size inequality, or the product formula, always rest on the fact that a non zero rational integer has absolute value at least 1.

Such a method yields the transcendence of values of f at points which do not belong to the restricted set. In general, it enables one to prove that some fields $\mathbb{Q}(\theta_1, \ldots, \theta_n)$ have transcendence degree ≥ 1 over $\mathbb{Q}$. Variants of this argument yield *measures of simultaneous approximation by algebraic numbers:* a quantitative refinement of the transcendence result is a lower bound for $\max_{1 \le i \le n} |\theta_i - \gamma_i|$, when $\gamma_1, \ldots, \gamma_n$ are algebraic numbers (such a lower bound depends explicitly on the degrees and heights of the algebraic numbers $\gamma_1, \ldots, \gamma_n$).

Here is an example of a measure of simultaneous approximation by algebraic numbers (see [97

([5]) We have the disposition of strong general zero estimates for commutative algebraic groups; see for instance Bertrand, Daniel – Lemmes de zéros et nombres transcendants. *Séminaire Bourbaki*, Vol. 1985/86. Astérisque No. **145-146** (1987), 3, 21–44.
In the proofs of the results stated in section 3 a result of P. Philippon plays a fundamental role. However, so far, apart from the setting of algebraic groups, the situation is not as good.

RW2]). We define the *absolute logarithmic height* of an algebraic number γ by

$$\mathrm{h}(\gamma) = \frac{1}{d}\log a_0 + \frac{1}{d}\sum_{i=1}^{d} \log \max\{1, |\gamma_i|\}$$

when the minimal polynomial $a_0 X^d + \cdots + a_d$ of γ over $\mathbb{Z}$ (with $a_0 > 0$) decomposes over $\mathbb{C}$ as

$$a_0 \prod_{i=1}^{d} (X - \gamma_i).$$

Proposition 2.1. *Let $\beta_1, \ldots, \beta_n$ be $\mathbb{Q}$-linearly independent algebraic numbers. There exists a positive constant $C = C(\beta_1, \ldots, \beta_n)$ such that, if $\gamma_1, \ldots, \gamma_n$ are algebraic numbers satisfying*

$$[\mathbb{Q}(\gamma_1, \ldots, \gamma_n) : \mathbb{Q}] \le D \quad \text{and} \quad \max_{1 \le i \le n} \mathrm{h}(\gamma_j) \le h$$

with $h \ge e$, then

$$|e^{\beta_1} - \gamma_1| + \cdots + |e^{\beta_n} - \gamma_n| \ge \exp\{-CD^{1+(1/n)} h (\log h + D \log D)(\log h + \log D)^{-1}\}.$$

In the case $n = 1$, it is not difficult to deduce from a measure of algebraic approximation for $\theta = \theta_1$ a *transcendence measure* of θ, i.e. a lower bound for $|P(\theta)|$, when $P \in \mathbb{Z}[X]$ is a non zero polynomial (this lower bound is explicit in terms of the degrees and heights of P). Conversely, from a transcendence measure one easily deduces a measure of approximation.

Now assume one wants to prove that some field $K = \mathbb{Q}(\theta_1, \ldots, \theta_n)$ has transcendence degree ≥ 2 (result of small transcendence degree). Assume not: if θ denotes any transcendence basis, then the field K is a finite extension of $\mathbb{Q}(\theta)$. Using the same scheme of proof as above, one constructs a number γ in K, and one meets a difficulty for the lower bound. One solution, suggested by S. Lang in 1966 (in his book on transcendental numbers), is to assume a transcendence measure for θ; such a transcendence measure needs to be rather sharp (the field $\mathbb{Q}(\theta)$ should have "finite transcendence type"). This suggests an inductive procedure for algebraic independence. However, so far, results obtained by this way are rather weak, partly because the Diophantine estimates which can be proved are far from the best possible ones. Also this method is not universal, since some numbers like Liouville ones will not satisfy the desired measure.

Another much more efficient solution arises from Gel'fond's work in 1949: the transcendence construction yields not only one element $\gamma \in K$, but a sequence γ_N of such elements. Instead of asking for a lower bound for each single γ_N, Gel'fond succeeded to prove that not all elements γ_N in this sequence can be too small.

One should point out that it is often possible to complete transcendence proofs (at least when they involve only functions of a single variable) without a sharp zero estimate, but for algebraic independence (as well as for quantitative results), one really needs precise zero estimates.

2.2. Criteria for Algebraic Independence and Measures

The proof of A.O. Gel'fond's criterion involved only elementary properties of resultants of two polynomials in a single variable. It enables one to prove that some fields have transcendence degree ≥ 2 over $\mathbb{Q}$. In few cases it shows that two numbers are algebraically independent (one such example is A.O. Gel'fond's solution of Conjecture 1.2 for $d = 3$). Several authors contributed to refine it

(see [84 W1]). Criteria for algebraic independence ("large transcendence degree") have been worked out by G.V. Chudnovsky (see Chap. 4 of [84 Chu]), E. Reyssat, R. Dvornicich, Yu.V. Nesterenko, P. Philippon, M. Waldschmidt and Zhu Yao Chen (see [84 W1]), as well as Zhu Yao Chen ([85 Z1], [89 Z1], [89 Z2], [90 Z]). One main tool, due to G.V. Chudnovsky, is the semi-resultant. These statements were sufficient to yield lower bounds for the transcendence degree of fields generated by values of the exponential function for instance, but these lower bounds were not sharp. The first sharp estimate has been announced by P. Philippon in [84 P] and proved in [86 P]. Here is Corollary 0.6 of [86 P] (the main result of [86 P] also splits degree and height; further statements and references are given in [98 NP]).

Theorem 2.2. (Philippon's Criterion for Algebraic Independence) *Let n be a positive integer, C a sufficiently large real number, $(\theta_1, \ldots, \theta_n)$ an element of $\mathbb{C}^n$ and η a positive real number. Assume that for all sufficiently large N, there exist a positive integer $m = m(N) \geq 1$ and polynomials $Q_1, \ldots, Q_m$ in $\mathbb{Z}[X_1, \ldots, X_n]$ with*

$$\max_{1\leq j\leq m} \deg Q_j \leq N, \qquad \max_{1\leq j\leq m} \mathrm{H}(Q_j) \leq e^N$$

and

$$0 < \max_{1\leq j\leq m} |Q_j(\theta_1, \ldots, \theta_n)| \leq e^{-CN^\eta},$$

such that the set of common zeros of the polynomials $Q_1, \ldots, Q_m$ in the ball

$$\left\{ z \in \mathbb{C}^n \,;\, \max_{1\leq i\leq n} |z_i - \theta_i| \leq e^{-3CN^\eta} \right\}$$

is finite. Then the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$ is $> \eta - 1$.

This statement allows one to give lower bounds for the transcendence degree of some fields. Quantitative refinements of such criteria have been studied by several authors: the goal is now to produce a result of Diophantine approximation, which includes the lower bound for the transcendence degree. When the conclusion of the proof of algebraic independence is that some numbers $\theta_1, \ldots, \theta_n$ are algebraically independent (an example is the Lindemann-Weierstraß Theorem, another one is A.O. Gel'fond's result on α^β and α^{β^2}; a few other examples are due to G.V. Chudnovsky), the most natural quantitative refinement is a lower bound for $|P(\theta_1, \ldots, \theta_n)|$, when P is a non zero polynomial with rational (or algebraic) coefficients. This is called a *measure of algebraic independence*. As shown by P. Philippon [85 P] and Yu.V. Nesterenko [85 Ne1], similar measures can also be given when the conclusion is only that the transcendence degree of the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$ over $\mathbb{Q}$ is greater than some number k which is $< n$. Another quantitative refinement is to give a lower bound for $\max_{1\leq i\leq n} |\theta_i - \gamma_i|$ when $\gamma_1, \ldots, \gamma_n$ belong to a field of transcendence degree $\leq k$; this is called a *measure of simultaneous approximation for $\theta_1, \ldots, \theta_n$*. An example with $k = 0$ is Proposition 2.1. In [85 P], P. Philippon compares both measures; he produces measures of algebraic independence and deduces measures of simultaneous approximations for various transcendental numbers.

In [88 Ab] and [89 Ab], M. Ably proves a criterion for measures of simultaneous approximation which yields sharper estimates than [85 P] for numbers of the form $e^{x_i y_j}$, α^{β^j}, and also for G.V. Chudnovsky's result on η/ω and π/ω. This later example is inspired by G. Philibert's result in [88 Ph] (see Theorem 3.1 below).

In [92 Jb], E.M. Jabbouri improves Philippon's results [85 P] and [86 P] and produces a criterion which yields effective measures of algebraic independence, splitting degree and height.

In order to prove general results for one parameter subgroups of commutative algebraic groups, M. Ably in [92 Ab2] combines the previous criteria for measures of algebraic independence [92 Jb] and measures of simultaneous approximation [89 Ab] into a single one. Finally C. Jadot [96 Jd] refines the previous criteria of algebraic independence due to P. Philippon and E.M. Jabbouri, so that he also includes criteria for linear independence due to Yu. V. Nesterenko, P. Bundschuh and T. Töpfer. Again Jadot's results are effective (i.e. his criterion can be used to produce measures of linear independence as well as measures of algebraic independence).

The reference [98 NP] contains an extensive exposition of the basic tools from commutative algebra and elimination theory, including *Chow forms*, which have been introduced by Yu.V. Nesterenko in this context. Following a lecture of D. Roy, we only give here the definition of *the Chow form associated with an algebraic variety* $V \subset \mathbb{P}_m(\overline{\mathbb{Q}})$ *of dimension* k *defined over the field* $\mathbb{Q}$ *of rational numbers*. Let

$$U_i = U_0^{(i)} X_0 + \cdots + U_m^{(i)} X_m \qquad (0 \le i \le k)$$

be generic linear forms. There exists an irreducible polynomial

$$F \in \mathbb{Q}[\underline{U}^{(0)}, \ldots, \underline{U}^{(k)}],$$

where $\underline{U}^{(i)}$ stands for the m-tuple $(U_0^{(i)}, \ldots, U_m^{(i)})$, such that, for any linear forms $L_0, \ldots, L_k$ in $\overline{\mathbb{Q}}[X_0, \ldots, X_m]$, say

$$L_i = u_0^{(i)} X_0 + \cdots + u_m^{(i)} X_m \qquad (0 \le i \le k)$$

the condition

$$F(\underline{u}^{(0)}, \ldots, \underline{u}^{(k)}) = 0$$

holds if and only if

$$L_0(\underline{x}) = \cdots = L_k(\underline{x}) = 0$$

have a solution $\underline{x}$ in V. This form F, which is unique up to a multiple in $\mathbb{Q}^\times$, is the *Chow form of* V.

2.3. Hilbert Nullstellensatz

The first results on large transcendence degree for values of elliptic functions are due to D.W. Masser and G. Wüstholz in the early 80's. They proved elliptic analog of Chudnovsky's result on the exponential function for elliptic functions with algebraic invariants without complex multiplication. In order to provide a replacement for the elimination technique of G.V. Chudnovsky by means of semi-resultants, they prove (and use) an explicit lower bound for the degree in Hilbert's Nullstellensatz. They need also tools from commutative algebra in order to refine their zero estimate. Another tool is an effective elliptic version of a Theorem of Kolchin on subgroups of products of algebraic groups.

The bounds of D.W. Masser and G. Wüstholz for the degree in Hilbert's Nullstellensatz were not sharp. W.D. Brownawell's succeeded to get essentially best possible estimates, by means of the powerful tools of Yu.V. Nesterenko and P. Philippon in elimination theory, as well as deep results from the theory of several complex variables of C. Berenstein and A. Yger. However, the method of Masser-Wüstholz then produces weaker results than Philippon's one in [86 P] (already in 1983 P. Philippon had much stronger results for large transcendence degree than those obtained by D.W. Masser and G. Wüstholz).

However an alternative approach to this question has been worked out by W.D. Brownawell in [89 Br]. He establishes sharp lower bounds for the maximum absolute values of integral polynomials having no common zero within a ball of given radius centered at a fixed point in $\mathbb{C}^n$. This allows him to relax the technical hypothesis: in place of a measure of linear independence, he only needs to assume that some lower bound holds for infinitely many values of the parameter. In [89 B], he works out the case of algebraic independence of values of the exponential function, or of elliptic functions without complex multiplication. The case of complex multiplication is considered in his joint paper with R. Tubbs [89 BT]. These two papers [89 B] and [89 BT] also give sharp effective quantitative measures of algebraic independence. Further references on this topic are [91 Tu] and [96 Den2].

2.4. Simultaneous Diophantine Approximation and Algebraic Independence

A new link between simultaneous approximation and algebraic independence arises from the work of D. Roy, M. Waldschmidt, M. Laurent, P. Philippon and G. Diaz (see [95 RW], [97 Di 2], [97 P], [97 RW1], [97 RW2], [98 LR2], [98 P1], [98 P2] and [98 P3]).

The basic idea is as follows. A complex transcendental number θ can be approximated by algebraic numbers. For instance Dirichlet's box principle enables one to produce a non zero polynomial $P \in \mathbb{Z}[X]$ such that $|P(\theta)|$ is small; then one considers the root of P which is closest to θ. This last step involves some technical complications, but E. Wirsing([6]) showed in 1961 how to overcome them. Denote by $\mathrm{M}(\gamma)$ *Mahler's measure* of the algebraic number γ, which is defined by

$$\mathrm{M}(\gamma) = e^{d\mathrm{h}(\gamma)}$$

where $d = [\mathbb{Q}(\gamma) : \mathbb{Q}]$ is the degree of γ.

Theorem 2.3. (Wirsing) *For any integer $D \geq 2$ there exist infinitely many algebraic numbers γ which satisfy*

$$[\mathbf{Q}(\gamma) : \mathbf{Q}] \leq D, \qquad \textit{and} \qquad |\theta - \gamma| \leq \mathrm{M}(\gamma)^{-D/4}.$$

Wirsing's arguments are related with Gel'fond's proof of his transcendence criterion. Apart from a result by H. Davenport and W.M. Schmidt (1968), the constant in Wirsing's result has not yet been substantially improved, but many useful recent variants have recently been produced. In [97 RW1] and [97 RW2], one considers more generally the simultaneous approximation of complex numbers by algebraic numbers. Given $\theta_1, \ldots, \theta_n$ in $\mathbb{C}$, one shows the existence of algebraic numbers $\gamma_1, \ldots, \gamma_n$ such that $\max |\theta_i - \gamma_i|$ is bounded from above in terms of the degree $\mathbb{Q}(\gamma_1, \ldots, \gamma_n)$, as well as the heights of γ_i's. The transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$ is the invariant which should, at least conjecturally, control the situation.

For instance, assume that the transcendence degree over $\mathbb{Q}$ of the field $K = \mathbb{Q}(\theta_1, \ldots, \theta_n)$ is 1. It is not too hard to check that an algebraic approximation of a single transcendental element in K will enable one to produce "simultaneous" algebraic approximations to $\theta_1, \ldots, \theta_n$. In other terms, if $\theta_1, \ldots, \theta_n$ have the property that they cannot be simultaneously approximated by algebraic numbers, then they cannot lie in a field of transcendence degree 1, and two at least of them are algebraically independent. This is how a link between simultaneous Diophantine approximation and algebraic independence arises.

Usually, "simultaneous" approximation (for instance of real numbers by rational ones) means that one has a good control of a common denominator of the rational approximations; more

([6]) Wirsing, Eduard – Approximation mit algebraischen Zahlen beschränkten Grades. J. reine angew. Math. **206** (1960), 67–77.

generally, "simultaneous" approximation of complex numbers by algebraic ones usually means that one has a good control of the absolute logarithmic height of the projective point whose coordinates are the algebraic approximations. Here, we do not pay too much attention to the constants, but we are interested with algebraic numbers of large degree, and we are concerned with bounds for the degree of the number field generated by the algebraic approximations.

The following statement is Conjecture 1.7 of [97 RW2].

Conjecture 2.4. – *Let $a \geq 1$, $b \geq 1$ be real numbers, t a non negative integer and $\theta_1, \ldots, \theta_n$ complex numbers. Let $\varphi : \mathbb{N} \times \mathbb{R}_+ \to \mathbb{R}_+ \cup \{\infty\}$ be a mapping with the following property: there exist a positive integer D_0 together with a real number $h_0 \geq 1$ such that, for any integer $D \geq D_0$, any real number $h \geq h_0$ and any n-tuple $(\gamma_1, \ldots, \gamma_n)$ of algebraic numbers satisfying*

$$[\mathbb{Q}(\gamma_1, \ldots, \gamma_n) : \mathbb{Q}] \leq D \quad \text{and} \quad \max_{1 \leq i \leq n} \mathrm{h}(\gamma_i) \leq h,$$

we have

$$\max_{1 \leq i \leq n} |\theta_i - \gamma_i| \geq \exp\bigl\{-\varphi(D, h)\bigr\}.$$

Let $(D_\nu)_{\nu \geq 1}$ be an increasing ([7]) sequence of positive integers and $(h_\nu)_{\nu \geq 1}$ an increasing sequence of positive real numbers with $D_\nu + h_\nu \to \infty$. Assume

$$D_{\nu+1} \leq aD_\nu, \qquad h_{\nu+1} \leq bh_\nu, \qquad (\nu \geq 1)$$

and

$$\limsup_{\nu \to \infty} \frac{1}{D_\nu^{1+(1/t)} h_\nu} \varphi(D_\nu, h_\nu) = 0$$

Then the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$ is $> t$.

So far, only the case $n = 1$ is solved, by M. Laurent and D. Roy [98 LR2].

Lindemann-Weierstraß Theorem on the algebraic independence of $e^{\beta_1}, \ldots, e^{\beta_n}$ (when $\beta_1, \ldots, \beta_n$ are $\mathbb{Q}$-linearly independent algebraic numbers) follows from Conjecture 2.4 and Proposition 2.1. The special case $n = 2$ (algebraic independence of e^{β_1} and e^{β_2}) follows from Proposition 2.1 together with the special case of Conjecture 2.4 which is proved in [97 RW2].

This approach yields results of algebraic independence (only small transcendence degree, so far) by means of Laurent's interpolation determinants. Previously, the method of interpolation determinants was limited to proofs involving only algebraic numbers: it was efficient only for showing that some fields have transcendence degree ≥ 1, as well as for providing quantitative versions of such results, namely measures of transcendence or of simultaneous algebraic approximation by algebraic numbers. The point is that such measures turn out to yield algebraic independence results!

Another solution to the problem of proving algebraic independence by means of interpolation determinants has been found by M. Laurent and D. Roy: in [98 LR1] they first extend Gel'fond's criterion by including multiplicities; next they show that the interpolation determinant produces a polynomial which, not only is small at some point, but also has small derivatives at that point.

In a forthcoming paper they also include derivatives in Philippon's criterion of algebraic independence. This will produce results of large transcendence degree by means of interpolation determinants. Unfortunately these new tools, which are definitely valuable from the point of view of the method, do not seem to produce new results which could not be reached by previous arguments, so far.

([7]) Increasing sequences are sometimes called non decreasing sequences: we do not exclude a constant sequence for instance.

Notice also that A. Sert's proof in [97 Se] of a measure of algebraic independence for $e^{\beta_1}, \dots, e^{\beta_n}$ (quantitative version of the Lindemann-Weierstraß Theorem) involves interpolation determinants. Another way of replacing the auxiliary function by an interpolation determinant has been worked out by P. Philippon in [97 P], [98 P1] and [98 P2]. One main difference between [97 RW1] and [97 P] is that Philippon considers approximation by algebraic cycles rather than by algebraic numbers. For instance, in the one dimensional case, given a transcendental number θ, instead of considering $|\theta - \gamma|$ for some algebraic number γ, he only needs to get a non zero polynomial $P \in \mathbb{Z}[X]$ such that $|P(\theta)|$ is small; and Dirichlet's box principle is just sufficient!

3. Gel'fond's Method and its Developments

3.1. Small Transcendence Degree

We start with "small transcendence degree". Many very interesting results are due to G.V. Chudnovsky [84 Chu], [84 W1]. We recall the following one: *Let $\mathcal{E}$ be an elliptic curve over $\overline{\mathbb{Q}}$, ω a non zero period of a differential form of first kind and η the corresponding period of a differential form of second kind. Then the two numbers ω/π and η/π are algebraically independent.*

Let ξ be an algebraic number and $\mathcal{E}$ the elliptic curve $y^2 = (1-x^2)(1-\xi x^2)$. In [96 An], Y. André states Chudnovsky's result in terms of values of hypergeometric functions, and gives a completely new proof by means of the Gel'fond-Dèbes method involving G-functions. Also he produces p-adic analog.

Here is an extension of G.V. Chudnovsky's result to Abelian varieties, due to K.G. Vasilev [96 V]. Let $F \in \overline{\mathbb{Q}}[X,Y]$ be an irreducible polynomial such that the curve $F(x,y) = 0$ has genus $g \geq 1$. Let $\varphi_1, \dots, \varphi_{2g}$ be differentials of first or second kind and $\gamma_1, \dots, \gamma_{2g}$ be closed integration paths on the Riemann surface such that the $2g \times 2g$ matrix

$$\Omega = \Big(\int_{\gamma_j} \varphi_i \Big)_{1 \leq i,j \leq 2g}$$

is non singular. Then *any $g+1$ rows of Ω contains at least 2 algebraically independent numbers.* As a consequence, *any subset with $[(n+1)/2]$ elements of the following set of values of the Beta function*

$$\big\{ B(k/n, 1/2)\,;\, 1 \leq k \leq n-1,\, k \neq n/2 \big\}$$

contains at least 2 algebraically independent numbers.

The fact that $\Gamma(1/4)$ and $\Gamma(1/3)$ are not Liouville numbers, which was claimed by G.V. Chudnovsky already in 1980 (see also [84 Chu] Th. 3 p. 18), has been proved only recently by P. Philippon in [98 P2]. More generally Philippon produces a sharp measure of algebraic independence of π/ω and η/ω:

Theorem 3.1. *Let $\wp$ be a Weierstraß elliptic function with algebraic invariants g_2, g_3. Let ω be a non zero period, and η be the corresponding quasi-period of the associated Weierstraß zeta function. There exists a constant $C > 0$ such that, for any non zero polynomial $P \in \mathbb{Z}[X,Y]$ of degree $\leq D$ and usual height $\leq H$,*

$$|P(\pi/\omega, \eta/\omega)| \geq \exp\big\{ -CD^2(\log H + D \log D) \big\}.$$

After Chudnovsky's pioneer work, previous weaker estimates had been obtained by G. Philibert in [88 Ph], by M. Ably in [89 Ab] and by E.M. Jabbouri in [92 Jb]. Notice that G. Philibert's

measure in [88 P] played an interesting role in connection with the work of P. Philippon related to the algebraic independence of π and e^π (see §4 below).

Gel'fond's algebraic independence Theorem (1949) on α^β and α^{β^2} has been extensively studied. The measure of algebraic independence he obtained with N.I. Feldman has been improved, especially by G. Diaz in [87 Di], [88 Di], [89 Di1] and [90 Di]; see also [90 She]. Here is the best known result by G. Diaz :

Theorem 3.2. *Let α be a non zero algebraic number, $\log\alpha$ a non zero logarithm of α and β a cubic number. There exists a constant $c > 0$ such that if $P \in \mathbb{Z}[X, Y]$ is a non zero polynomial of degree $\leq D$ and usual height $\leq H$, then*

$$\log\big|P(\alpha^\beta, \alpha^{\beta^2})\big| \geq -\exp\big\{cD(D + \log H)\big\}.$$

The elliptic analog of Gel'fond's Theorem on α^β and α^{β^2}, announced by D.W. Masser and G. Wüstholz in the early 80's, has been proved in [86 MW]. Much sharper results have then been achieved by P. Philippon in 1983. In [86 Tu2], R. Tubbs gives a lower bound for $|P\big(\wp(\beta u), \wp(\beta^2 u)\big)|$ in the CM case (here, $\wp$ is an elliptic function of Weierstraß with algebraic invariants and complex multiplication, u is a complex number such that $\wp(u)$ is algebraic, P a polynomial with rational integer coefficients and β is an algebraic number of degree 3 over the field of complex multiplications). In [88 Tu], he removes the assumption that $\wp(u)$ is algebraic and produces a lower bound for pairs of relatively prime integral polynomials evaluated at $\big(\wp(u), \wp(\beta u), \wp(\beta^2 u)\big)|$ (elliptic analog of a result of W.D. Brownawell in 1979). The elliptic analog of Theorem 3.2 has been established by S.O. Shestakov [92 She]. For an updated survey of such questions with new results, see [96 Ca].

General results of small transcendence degree related with one parameter subgroups of commutative algebraic groups are obtained in [85 W]. The main difference with [86 W] is that no technical hypothesis is needed for small transcendence degree. These results do not exhaust the possibilities of the method: some results by G.V. Chudnovsky [84 Chu] are not covered by the statements of [85 W] and many variations are possible (see for instance the papers [86 TY] by M. Toyoda and T. Yasuda and [86 Tu1], [87 Tu1] by R. Tubbs). A more systematic study has been achieved by R. Tubbs in [87 Tu2] and [90 Tu2]. Further results related to Baker's method (see Chap. 2 of [84 Chu]) are due to G. Diaz [92 Di].

Transcendence measures enable one to construct algebraically independent numbers: an early example is due to N.I. Feldman (1964): using a lower bound for $|\beta - \log\alpha|$ when α and β are algebraic numbers, he proved that for some "Liouville" numbers a, the two numbers a and e^a are algebraically independent. Here, "Liouville" number means a complex number a which is very well approximated by rational, or more generally algebraic, numbers.

In the same way, R. Tubbs [90 Tu1] uses a lower bound for elliptic linear forms in logarithms and proves, for algebraic β, the algebraic independence of u and $\wp(\beta u)$ for some Liouville numbers u, and also the algebraic independence of $\wp(u)$ and $\wp(\beta u)$ for some complex numbers u such that $\wp(u)$ is Liouville. In [93 Ca], D. Caveny shows the algebraic independence of a and a^b when a and b are Liouville numbers; with R. Tubbs in [93 CT] they refine Fel'dman's above mentioned result on a and e^a and also discuss the elliptic analog. Using a lower bound for linear forms in logarithms, D. Caveny gets in [94 Ca] the algebraic independence of a and a^β for a Liouville number a and an algebraic β. A similar elliptic situation is considered by M. Ably in [91 Ab].

Usually, each single recent paper deals with either transcendence degree ≥ 2 or else large transcendence degree. One of the few exceptions are [89 Tu] where R. Tubbs produces fields of transcendence degree ≥ 3 generated by values of an elliptic function, and [98 P2].

We conclude this section with a partial result concerning Conjecture 1.5. It is still not proved that the field generated by all the logarithms of algebraic numbers has transcendence degree ≥ 2 over $\mathbb{Q}$: it might just as well be an algebraic extension of $\mathbb{Q}(\pi)$ (but this would be unexpected!). One of the very few known results in this direction arises from [97 RW1] and [97 RW2]:

Theorem 3.3. *Let $\ell_1, \ldots, \ell_n$ be $\mathbb{Q}$-linearly independent elements of $\mathcal{L}$. Assume that the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\ell_1, \ldots, \ell_n)$ is 1. Then for each non zero homogeneous polynomial $Q \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree 2 (quadratic form), the number $Q(\ell_1, \ldots, \ell_n)$ does not vanish.*

3.2. Large Transcendence Degree

In [84 W1], we noticed that Philippon's results on the elliptic analog of the Gel'fond-Schneider problem were stronger than the exponential result. Shortly after, P. Philippon succeeded to prove the expected result in the exponential case.

Let t be the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}\big(\alpha^\beta, \alpha^{\beta^2}, \ldots, \alpha^{\beta^{d-1}}\big)$. After the works of G.V. Chudnovsky, P. Warkentin, P. Philippon, E. Reyssat, R. Endell, W.D. Brownawell and Yu.V. Nesterenko (see [84 W1] as well as [84 Ne1]), the best known lower estimate for t was

$$2^t > \frac{d+1}{2}.$$

In 1984 P. Philippon succeeded to reach the lower bound $t \geq (d-1)/2$, which can be written $t \geq [d/2]$ where [ ] denotes the integral part. In [84 P] he announced the result, together with a sharp criterion for algebraic independence, as well as a quantitative refinement (measure of algebraic independence) whic