Madras Number Theory Symposium February 22, 1997
The Ramanujan Journal

Simultaneous Approximation and Algebraic Independence

by Damien ROY[(*)] and Michel WALDSCHMIDT

Introduction

For a complex number θ, Dirichlet's box principle provides a polynomial with rational integer coefficients whose value at the point θ is "small". If the number θ is algebraic, this polynomial may be a multiple of the minimal polynomial of θ over $\mathbb{Z}$. On the other hand, if θ is transcendental, one gets an algebraic approximation to θ by taking a root of this polynomial. More generally, when $\theta_1, \ldots, \theta_n$ are complex numbers in a field of transcendence degree 1 over $\mathbb{Q}$, it is possible to construct sequences $(\gamma_1^{(N)}, \ldots, \gamma_n^{(N)})$, $(N \geq 1)$ of simultaneous algebraic approximations to $\theta_1, \ldots, \theta_n$. Therefore if we can prove for $\theta_1, \ldots, \theta_n$ a sharp measure of simultaneous approximation, namely if we can bound from below the quantity $\max_{1 \leq i \leq n} |\theta_i - \gamma_i|$ in terms of the heights of γ_i and the degree of the number field $\mathbb{Q}(\gamma_1, \ldots, \gamma_n)$, one deduces that at least two of the numbers θ_i are algebraically independent.

This argument enables one to deduce algebraic independence results from diophantine estimates without using Gel'fond's transcendence criterion. We develop this point of view by considering a few examples. For instance we deduce Gel'fond's result, which states that the two numbers $2^{\sqrt[3]{2}}$ and $2^{\sqrt[3]{4}}$ are algebraically independent, from the following diophantine estimate: *if γ_1 and γ_2 are algebraic numbers with bounded absolute logarithmic height, and if D denotes the degree of the number field $\mathbb{Q}(\gamma_1, \gamma_2)$ over $\mathbb{Q}$, then*

$$|2^{\sqrt[3]{2}} - \gamma_1| + |2^{\sqrt[3]{4}} - \gamma_2| > \exp\{-CD^2(\log D)^{-1/2}\},$$

where the constant C depends only on the heights of the numbers γ_1 and γ_2. The main point in this lower bound is that the function inside the exponent is bounded by $o(D^2)$.

[(*)] `Work of this author partially supported by NSERC and CICMA`

In the first section, we produce a criterion which yields the algebraic independence of two numbers, provided that they satisfy a suitable measure of simultaneous approximation. In section 2 we consider values of the usual exponential function: for numbers of the shape $e^{x_i y_j}$, we obtain a measure of simultaneous approximation, assuming that the complex numbers x_i as well as y_j satisfy a "technical" condition (namely a measure of linear independence). This technical hypothesis cannot be omitted, as we show with an example involving Liouville numbers. Also in section 2 we give a diophantine estimate related to the Lindemann-Weierstraß theorem: *for $\mathbb{Q}$-linearly independent algebraic numbers $\beta_1, \dots, \beta_n$, there exists a positive constant $C = C(\beta_1, \dots, \beta_n)$ such that, if $\gamma_1, \dots, \gamma_n$ are algebraic numbers satisfying*

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

then

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

The best known measures of simultaneous approximation for pairs of numbers like (π, e^π), or (e, π), are not yet sufficient to deduce algebraic independence. The same is true for $\mathbb{Q}$-linearly independent logarithms of algebraic numbers $\log \alpha_1, \dots, \log \alpha_n$. However we get a sufficiently sharp estimate which implies a result of algebraic independence if we assume that there exists a nonzero homogeneous quadratic polynomial Q which vanishes at the point $(\log \alpha_1, \dots, \log \alpha_n)$: under this assumption, we prove that for algebraic numbers $\gamma_1, \dots, \gamma_n$ with logarithmic height $\le \log D$ in a field of degree $\le D$ over $\mathbb{Q}$, we have

$$\sum_{j=1}^{n} \bigl|\log \alpha_j - \gamma_j\bigr| \ge e^{-CD^2},$$

where C depends only on $\log \alpha_1, \dots, \log \alpha_n$ and Q.

The next section (§ 3) deals with elliptic functions. We replace the usual exponential function $\exp(z) = e^z$ by a Weierstraß elliptic function $\wp$. Finally in section 4 we propose a measure of simultaneous approximation for the two numbers π and $\Gamma(1/4)$ by algebraic numbers of bounded absolute logarithmic height:

$$|\pi - \gamma_1| + |\Gamma(1/4) - \gamma_2| > \exp\{-CD^{3/2} \log D\}.$$

The second part of this paper (§§ 5 to 11) includes the proofs.

Here we consider only complex numbers, but the same method yields diophantine approximation estimates as well as results of algebraic independence for p-adic fields also.

`Aknowledgement.` We are thankful to Deanna Caveny for her comments on a preliminary broken English version of this text.

§1. Simultaneous approximation of complex numbers

a) Algebraic approximation to a complex number

Let θ be a complex number. Using Dirichlet's box principle, we deduce that for any integer $D \geq 1$ and any real number $H \geq 1$, there exists a nonzero polynomial $f \in \mathbb{Z}[X]$, of degree $\leq D$ and usual height (maximum absolute value of its coefficients) $\leq H$, such that

$$|f(\theta)| \leq \sqrt{2}\big(1 + |\theta| + \cdots + |\theta|^D\big)H^{-(D-1)/2}.$$

We shall keep in mind only the weaker assertion: *for any $\theta \in \mathbb{C}$, there exist three positive constants D_0, H_0 and c_1 such that, for any $D \geq D_0$ and any $H \geq H_0$, there exists a polynomial $f \in \mathbb{Z}[X]$, $f \neq 0$, of degree $\leq D$ and usual height $\leq H$ satisfying*

$$|f(\theta)| \leq e^{-c_1 D \log H}$$

(admissible values are $D_0 = 2$, $H_0 = 18^5 \max\{1, |\theta|\}^{20}$ and $c_1 = 1/5$).

On the other hand, if the number θ is algebraic, one deduces from Liouville's inequality that for any nonzero polynomial $f \in \mathbb{Z}[X]$ of degree $\leq D$ and usual height $\leq H$, either $f(\theta) = 0$, or else

$$|f(\theta)| \geq e^{-c_2(D + \log H)},$$

with $c_2 = d + \log H(\theta)$, where d denotes the degree of θ and $H(\theta)$ its usual height (which is the usual height of its minimal polynomial over $\mathbb{Z}$). Therefore, provided D and H are sufficiently large, the polynomial which arises from the pigeonhole principle vanishes at θ (assuming θ is algebraic).

Liouville's inequality can be phrased in terms of diophantine approximation by algebraic numbers: *if θ is an algebraic number, there exists a constant $c_3 > 0$ such that, for any algebraic number γ of degree $\leq D$ and usual height $\leq H$ with $\gamma \neq \theta$, the inequality*

$$|\theta - \gamma| \geq e^{-c_3(D + \log H)}$$

holds.

Sometimes it is more convenient to use the absolute logarithmic height $\mathrm{h}(\gamma)$ instead of the usual height $H(\gamma)$: if the minimal polynomial of γ over $\mathbb{Z}$ is

$$a_0 X^d + a_1 X^{d-1} + \cdots + a_{d-1} X + a_d = a_0 \prod_{j=1}^{d} (X - \gamma_j)$$

with $d = [\mathbb{Q}(\gamma) : \mathbb{Q}]$ and $a_0 > 0$, *Mahler's measure* of γ is

$$\mathrm{M}(\gamma) = a_0 \prod_{j=1}^{d} \max\{1, |\gamma_j|\},$$

and the *absolute logarithmic height* of γ is

$$\mathrm{h}(\gamma) = \frac{1}{d}\log \mathrm{M}(\gamma).$$

In order to get an upper bound for $\mathrm{h}(\gamma)$, we need an upper bound for $\mathrm{M}(\gamma)$, and a *lower* bound for d. This is the reason why we use different letters to denote the exact degree d of γ and an upper bound D for the same degree. Using the estimates

$$2^{-d}H(\gamma) \le \mathrm{M}(\gamma) \le H(\gamma)\sqrt{d+1},$$

we deduce (cf. [32], Lemma 3.11)

$$\frac{1}{d}\log H(\gamma) - \log 2 \le \mathrm{h}(\gamma) \le \frac{1}{d}\log H(\gamma) + \frac{1}{2d}\log(d+1).$$

Liouville's inequality (see for instance [9], Lemma 9.2, and [32], Lemma 3.14) gives

$$|\theta-\gamma| \ge \exp\bigl\{-\delta\bigl(\mathrm{h}(\gamma)+\mathrm{h}(\theta)+\log 2\bigr)\bigr\}$$

with $\delta = [\mathbb{Q}(\gamma,\theta):\mathbb{Q}]$. We set $d = [\mathbb{Q}(\gamma):\mathbb{Q}]$ and $d_0 = [\mathbb{Q}(\theta):\mathbb{Q}]$. Hence we have $\delta \le d_0 d$ and

$$|\theta-\gamma| \ge \exp\bigl\{-c_4 d\bigl(\mathrm{h}(\gamma)+1\bigr)\bigr\},$$

with $c_4 = d_0\max\{1, \mathrm{h}(\theta)+\log 2\}$. Therefore we can choose $c_3 = (3/2)c_4$. Finally, if we define $c_5 = 2c_4$, we conclude:

Liouville's inequality. *If θ is an algebraic number, there exists a positive constant c_5 such that, for any rational integer $D \ge 1$ and any real number $h \ge 1$, if γ is an algebraic number, distinct from θ, of degree $\le D$ and absolute logarithmic height $\mathrm{h}(\gamma) \le h$, then*

$$|\theta-\gamma| \ge \exp\bigl\{-c_5 Dh\bigr\}.$$

We now consider the approximation of a *transcendental* complex number by algebraic numbers.

Definition. Let θ be a complex number. A function $\varphi : \mathbb{N}\times\mathbb{R}_+ \to \mathbb{R}_+\cup\{\infty\}$ is an *approximation measure for* θ if there exist a positive integer D_0 and a real number $h_0 \ge 1$ such that, for any rational integer $D \ge D_0$, any real number $h \ge h_0$ and any algebraic number γ satisfying

$$[\mathbb{Q}(\gamma):\mathbb{Q}] \le D \quad \text{and} \quad \mathrm{h}(\gamma) \le h,$$

the following inequality holds:

$$|\theta-\gamma| \ge \exp\bigl\{-\varphi(D,h)\bigr\}.$$

This definition is slightly different from the corresponding one in [29], but is more convenient for our present purpose. We allow the value ∞ for φ so that algebraic numbers are not excluded. The condition $D \geq D_0$ is unimportant (algebraic numbers of small degree are not excluded). However, by assuming $h \geq h_0$, we do not take into account some refinements which may occur when one considers the approximation of complex numbers by algebraic numbers of small absolute height (for instance by algebraic numbers of bounded Mahler's measure).

Examples.

Here are a few approximation measures which are known for various transcendental numbers.

- The following approximation measure for π is due to N.I. Fel'dman (Theorem 5.7 of [9], Chap. 7, p.120). An explicit value for the constant C is produced in [29], Theorem 3.1 and [18], Theorem 2.

  There exists an absolute constant C such that the function

$$CD^2(h + \log D)\log D$$

  is an approximation measure for the number π.

- Let α be a nonzero algebraic number and $\log\alpha$ a nonzero determination of its logarithm. Again N.I. Fel'dman (Theorem 8.7 of [9], Chap. 7, p.135) proved an approximation measure for $\log\alpha$. An explicit value for $C = C(\log\alpha)$ is given in [29], Theorem 3.6 and [18], Theorem 5b.

  There exists a constant $C = C(\log\alpha)$ such that the function

$$CD^3(h + \log D)(\log D)^{-1}$$

  is an approximation measure for $\log\alpha$.

- Let β be a nonzero algebraic number. The best known approximation measure for e^β is due to G. Diaz [8], Cor. 2 (a refinement of the explicit constant $C = C(\beta)$ is given in [18], Theorem 5a):

  There exists a constant $C = C(\beta)$ such that the function

$$CD^2h(\log h + D\log D)(\log h + \log D)^{-1}$$

  is an approximation measure for the number e^β.

Other approximation measures are given in [29] and in [6] (see especially [6], Theorem 2.4, p.41, Theorems 2.5, 2.7 and 2.8, p.45 and Theorem 2.10, p.47, for the numbers e, e^{π} and α^{β}).

A natural question is to ask *what is the best possible approximation measure for a transcendental number?* One expects that a function whose growth rate is slower than D^2h cannot be an approximation measure (compare with conjecture 1.7 below). In terms of the usual height, this limit corresponds to the function $D\log H$. The first precise statement in this direction is due to Wirsing ([34], inequality (4')):

Let θ be a transcendental complex number. For any rational integer $D \geq 2$ there exist infinitely many algebraic numbers γ satisfying

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

Here is a variant of Wirsing's result which is proved in [21], théorème 3.2.

Theorem 1.1. – *Let θ be a transcendental number and φ an approximation measure for θ. Then, for sufficiently large h,*

$$\limsup_{D\to\infty} \frac{1}{D^2}\varphi(D,h) \geq 10^{-7}h.$$

Here is the main idea of the proof for Theorem 1.1 as well as for Wirsing's theorem. We start from a polynomial produced by Dirichlet's pigeonhole principle and we select a root at minimal distance from θ. The arguments are similar to those which occur in the proof of Gel'fond's criterion ([11], chap. III, § 4, Lemma VII, p.148). In fact, this criterion of Gel'fond has been formulated by Brownawell in terms of algebraic approximation to a complex number ([5], Theorem 2).

b) Simultaneous approximation of several complex numbers

In the previous subsection we considered the approximation to a single complex number θ. Now we consider simultaneous approximation to numbers $\theta_1,\ldots,\theta_n$. We first extend the definition of approximation measure to the case of several numbers.

Definition. Let $\theta_1,\ldots,\theta_n$ be complex numbers. A function $\varphi:\mathbb{N}\times\mathbb{R}_+\to\mathbb{R}_+\cup\{\infty\}$ is a *measure of simultaneous approximation for* $\theta_1,\ldots,\theta_n$ if there exists 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

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

There exists a finite measure of simultaneous approximation for the numbers $\theta_1,\ldots,\theta_n$ provided they are not all algebraic.

An alternative definition consists of replacing $\max_{1\le i\le n} \mathrm{h}(\gamma_i)\le h$ by an upper bound for the height of the projective point $(1:\gamma_1:\cdots:\gamma_n)$ (see for instance [32], Chap. 3, § 2). However, for our present purpose, this does not make a difference, since

$$\max_{1\le i\le n} \mathrm{h}(\gamma_i) \le \mathrm{h}(1:\gamma_1:\cdots:\gamma_n) \le \mathrm{h}(\gamma_1)+\cdots+\mathrm{h}(\gamma_n).$$

It makes a difference only when sharp estimates for the constants are considered, like in the work of Schmidt.

Examples. Measures of simultaneous approximation are given in [9], [16], [22] and [23]. We shall see several other examples. To begin with, here is a result due to N.I. Fel'dman ([9], Theorem 7.7, p.128).

Let $\alpha_1,\ldots,\alpha_n$ be nonzero algebraic numbers. For $1\le i\le n$, let $\log\alpha_i$ be a determination of the logarithm of α_i. Assume the numbers $\log\alpha_1,\ldots,\log\alpha_n$ are $\mathbb{Q}$-linearly independent. Then there exists a positive constant C such that

$$CD^{2+1/n}(h+\log D)(\log D)^{-1}$$

is a measure of simultaneous approximation for the numbers $\log\alpha_1,\ldots,\log\alpha_n$.

For $n=1$ we recover Fel'dman's above mentioned approximation measure for the number $\log\alpha$.

We shall deduce from Theorem 1.1 the following corollary.

Corollary 1.2. – *Let $\theta_1,\ldots,\theta_n$ be complex numbers and $\varphi:\mathbb{N}\times\mathbb{R}_+\to\mathbb{R}_+$ a measure of simultaneous approximation for $\theta_1,\ldots,\theta_n$. Assume*

$$\liminf_{h\to\infty}\frac{1}{h}\limsup_{D\to\infty}\frac{1}{D^2}\varphi(D,h)=0.$$

Then the field $\mathbb{Q}(\theta_1,\ldots,\theta_n)$ has transcendence degree ≥ 2 over $\mathbb{Q}$.

In the next section (§ 2 below) we shall show by an example that this sufficient condition is not necessary: there exist fields of transcendence degree 2 which are generated by complex numbers $\theta_1,\ldots,\theta_n$ which are simultaneously very well-approximated by algebraic numbers.

c) Specialization lemma

We deduce Corollary 1.2 from Theorem 1.1. It is plainly sufficient to prove the following result.

Proposition 1.3. – *Let n and m be positive integers with $1 \leq n \leq m$ and let $\theta_1, \ldots, \theta_m$ be complex numbers. Assume that $\theta_{n+1}, \ldots, \theta_m$ are algebraic over the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$. Under these assumptions, there exist three positive constants $c_0 \in \mathbb{R}$, $c_1 \in \mathbb{N}$ and $c_2 \in \mathbb{R}$, which depend only on $\theta_1, \ldots, \theta_m$, such that, if $\varphi(D, h)$ is a simultaneous approximation measure for these m numbers, then $c_0 + \varphi(c_1 D, c_2 h)$ is a simultaneous approximation measure for $\theta_1, \ldots, \theta_n$.*

Roughly speaking, Proposition 1.3 means that, up to constants, a simultaneous approximation measure depends only on a transcendence basis of the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$.

The proof of Proposition 1.3 will rest on several preliminary lemmas.

Lemma 1.4. – *Let*

$$f(T) = a_0 T^d + \cdots + a_d = a_0 (T - \zeta_1) \cdots (T - \zeta_d)$$

be a polynomial with complex coefficients and degree $d \geq 1$. Assume f is separable (i.e. has no multiple root). There exist two positive constants $c = c(f)$ and $\eta = \eta(f)$ such that, if $\tilde{a}_0, \ldots, \tilde{a}_d$ are complex numbers satisfying

$$\max_{0 \leq i \leq d} |a_i - \tilde{a}_i| < \eta,$$

then the polynomial

$$\tilde{f}(T) = \tilde{a}_0 T^d + \cdots + \tilde{a}_d$$

can be written

$$\tilde{f}(T) = \tilde{a}_0 (T - \tilde{\zeta}_1) \cdots (T - \tilde{\zeta}_d)$$

with

$$\max_{1 \leq j \leq d} |\zeta_j - \tilde{\zeta}_j| \leq c \max_{0 \leq i \leq d} |a_i - \tilde{a}_i|.$$

Proof. (Compare with [10], Chap. I, Lemma 8.7 and Corollary 8.8.)

We shall obtain explicit values for η and c. Set

$$r = \frac{1}{2} \min_{i \neq j} |\zeta_i - \zeta_j|, \qquad r_0 = \max\{|\zeta_1|, \ldots, |\zeta_d|\}, \qquad R = \max\{1, r + r_0\}$$

and define

$$\eta = \frac{|a_0| r^d}{(d+1) R^d}, \qquad c = r/\eta.$$

For $|z| \leq R$, we have

$$|f(z) - \tilde{f}(z)| \leq \max_{0 \leq i \leq d} |a_i - \tilde{a}_i| (1 + R + \cdots + R^d) < |a_0| r^d.$$

For $|z-\zeta_i|=r$, we have

$$|f(z)| = |a_0|\prod_{j=1}^d |z-\zeta_j| \geq |a_0|r^d.$$

According to Rouché's theorem, since the estimate $|f(z)-\tilde{f}(z)|<|f(z)|$ holds for z on the circumference of the disk $|z-\zeta_i|\leq r$, the two functions f and $\tilde{f}$ have the same number of zeroes in this open disk. Hence $\tilde{f}$ has a single zero $\tilde{\zeta}_i$ in the same disk. For $i\neq j$, according to the definition of r, we also have $|\tilde{\zeta}_j-\zeta_i|\geq r$. Therefore

$$|f(\tilde{\zeta}_j)| = |a_0|\prod_{i=1}^d |\tilde{\zeta}_j-\zeta_i| \geq |a_0|r^{d-1}|\tilde{\zeta}_j-\zeta_j|.$$

On the other hand

$$|f(\tilde{\zeta}_j)| = |f(\tilde{\zeta}_j)-\tilde{f}(\tilde{\zeta}_j)| \leq \max_{0\leq i\leq d}|a_i-\tilde{a}_i|(d+1)R^d.$$

This completes the proof of Lemma 1.4. □

Lemma 1.5. – *Let $P\in\mathbb{Z}[Y_1,\ldots,Y_m]$ be a polynomial in m variables of degree D_j in Y_j, $(1\leq j\leq m)$. Let $\gamma_1,\ldots,\gamma_m$ be algebraic numbers. Then*

$$\mathrm{h}\bigl(P(\gamma_1,\ldots,\gamma_m)\bigr) \leq \log \mathrm{L}(P) + \sum_{j=1}^m D_j \mathrm{h}(\gamma_j).$$

Proof. See for instance [32], Lemma 3.6.

Lemma 1.6. – *Let $F\in\mathbb{Z}[X_1,\ldots,X_n,T]$ be a polynomial in $n+1$ variables of degree D_j in X_j, $(1\leq j\leq n)$, and let $\alpha_1,\ldots,\alpha_n$, β be algebraic numbers which satisfy $F(\alpha_1,\ldots,\alpha_n,\beta)=0$. Assume that $F(\alpha_1,\ldots,\alpha_n,T)\in\mathbb{Q}(\alpha_1,\ldots,\alpha_n)[T]$ is not the zero polynomial. Then*

$$\mathrm{h}(\beta) \leq 2\log \mathrm{L}(F) + 2\sum_{j=1}^n D_j \mathrm{h}(\alpha_j).$$

Proof. (We are thankful to Guy Diaz who kindly provided us with the following proof).

Let t be the degree of F in the variable T. Write $\underline{\alpha}$ for $(\alpha_1,\ldots,\alpha_n)$, $\underline{X}$ for $(X_1,\ldots,X_n)$, and write

$$F(\underline{X},T) = T^tQ_t(\underline{X}) + T^{t-1}Q_{t-1}(\underline{X}) + \cdots + Q_0(\underline{X}).$$

Since $F(\underline{\alpha},T)\in\mathbb{Q}(\underline{\alpha})[T]$ is not the zero polynomial and since $F(\underline{\alpha},\beta)$ vanishes, at least one of the numbers $Q_t(\underline{\alpha}),\ldots,Q_1(\underline{\alpha})$ does not vanish. Denote by m the largest index j, $(1\leq j\leq m)$ such that $Q_j(\underline{\alpha})\neq 0$. From $F(\underline{\alpha},\beta)=0$ we deduce

$$-\beta^mQ_m(\underline{\alpha}) = \beta^{m-1}Q_{m-1}(\underline{\alpha}) + \cdots + \beta Q_1(\underline{\alpha}) + Q_0(\underline{\alpha}).$$

Define

$$\tilde{Q}(\underline{X},T) = T^{m-1}Q_{m-1}(\underline{X}) + \cdots + TQ_1(\underline{X}) + Q_0(\underline{X}),$$

so that

$$-\beta^m Q_m(\underline{\alpha}) = \tilde{Q}(\underline{\alpha},\beta).$$

An upper bound for $\mathrm{h}(\beta^m)$ is

$$\mathrm{h}(\beta^m) = \mathrm{h}\big(\beta^m Q_m(\underline{\alpha})Q_m(\underline{\alpha})^{-1}\big) \le \mathrm{h}\big(\beta^m Q_m(\underline{\alpha})\big) + \mathrm{h}\big(Q_m(\underline{\alpha})\big) = \mathrm{h}\big(\tilde{Q}(\underline{\alpha},\beta)\big) + \mathrm{h}\big(Q_m(\underline{\alpha})\big).$$

Using Lemma 1.5, we bound $\mathrm{h}\big(\tilde{Q}(\underline{\alpha},\beta)\big)$ and $\mathrm{h}\big(Q_m(\underline{\alpha})\big)$ from above:

$$\mathrm{h}\big(Q_m(\underline{\alpha})\big) \le \log \mathrm{L}(Q_m) + \sum_{j=1}^n (\deg_{X_j} Q_m)\mathrm{h}(\alpha_j)$$

and

$$\mathrm{h}\big(\tilde{Q}(\underline{\alpha},\beta)\big) \le \log \mathrm{L}(\tilde{Q}) + \sum_{j=1}^n (\deg_{X_j} \tilde{Q})\mathrm{h}(\alpha_j) + (\deg_T \tilde{Q})\mathrm{h}(\beta).$$

The degrees $\deg_{X_j} Q_m$ and $\deg_{X_j} \tilde{Q}$ are bounded by $\deg_{X_j} F = D_j$. Also we have $\deg_T \tilde{Q} \le m-1$. Coming back to $\mathrm{h}(\beta^m)$, we deduce

$$m\mathrm{h}(\beta) = \mathrm{h}(\beta^m) \le \log \mathrm{L}(Q_m) + \log \mathrm{L}(\tilde{Q}) + 2\sum_{j=1}^n D_j \mathrm{h}(\alpha_j) + (m-1)\mathrm{h}(\beta).$$

Hence

$$\mathrm{h}(\beta) \le \log \mathrm{L}(Q_m) + \log \mathrm{L}(\tilde{Q}) + 2\sum_{j=1}^n D_j \mathrm{h}(\alpha_j).$$

Since $\mathrm{L}(Q_m) + \mathrm{L}(\tilde{Q}) \le \mathrm{L}(F)$, we see that $\log \mathrm{L}(Q_m) + \log \mathrm{L}(\tilde{Q})$ is bounded by $2\log \mathrm{L}(F)$, which yields the desired estimate. □

Remark. The proof of Lemma 5 in [2] (which deals with the case $n=1$) yields, under the assumptions of Lemma 1.6, the following upper bound for Mahler's measure of β:

$$\mathrm{M}(\beta) \le \mathrm{L}(F)^d \prod_{j=1}^n \mathrm{M}(\alpha_j)^{D_j},$$

where $d = [\mathbb{Q}(\alpha_1,\ldots,\alpha_n):\mathbb{Q}]$. The advantage of Lemma 1.6 is to produce an upper bound for $\mathrm{h}(\beta)$ which does not depend on d.

Proof of Proposition 1.3. By induction, it is sufficient to deal with the case $m = n+1$. Write $\underline{\theta}$ for $(\theta_1,\ldots,\theta_n)$. Let $F \in \mathbb{Z}[X_1,\ldots,X_n,T]$ be a nonzero polynomial of degree d

in T such that $f(T)=F(\underline{\theta},T)\in\mathbb{C}[T]$ is separable, of degree d, and has θ_{n+1} as a root. Denote by η and c the constants related to f by Lemma 1.4. Write

$$F(X_1,\ldots,X_n,T)=\sum_{j=0}^{d}a_j(X_1,\ldots,X_n)T^{d-j}.$$

There exists a positive constant c_3 such that, for any $\underline{\theta}'=(\theta_1',\ldots,\theta_n')\in\mathbb{C}^n$ satisfying $\max_{1\le i\le n}|\theta_i-\theta_i'|\le 1$, we have

$$\max_{0\le j\le d}\bigl|a_j(\underline{\theta})-a_j(\underline{\theta}')\bigr|\le c_3\max_{1\le i\le n}|\theta_i-\theta_i'|.$$

Since $a_0(\underline{\theta})\ne 0$, there exists a positive constant c_4 such that $a_0(\underline{\theta}')\ne 0$ for $\max_{1\le i\le n}|\theta_i-\theta_i'|\le c_4$.

Let $\gamma_1,\ldots,\gamma_n$ be algebraic numbers, D a positive integer and $h\ge 1$ a real number such that

$$\max_{1\le i\le n}\mathrm{h}(\gamma_i)\le h,\quad [\mathbb{Q}(\gamma_1,\ldots,\gamma_n):\mathbb{Q}]\le D\quad\text{ and }\quad\max_{1\le i\le n}|\theta_i-\gamma_i|<\min\{1,\eta/c_3,c_4\}.$$

Since $a_0(\gamma_1,\ldots,\gamma_n)\ne 0$, we have $F(\gamma_1,\ldots,\gamma_n,T)\ne 0$. Using Lemma 1.4 we see that the polynomial $F(\gamma_1,\ldots,\gamma_n,T)$ has a root γ_{n+1} which satisfies

$$|\theta_{n+1}-\gamma_{n+1}|\le c_5\max_{1\le i\le n}|\theta_i-\gamma_i|$$

with $c_5=\max\{1,cc_3\}$. Since

$$[\mathbb{Q}(\gamma_1,\ldots,\gamma_n,\gamma_{n+1}):\mathbb{Q}(\gamma_1,\ldots,\gamma_n)]\le d,$$

we have $[\mathbb{Q}(\gamma_1,\ldots,\gamma_n,\gamma_{n+1}):\mathbb{Q}]\le dD$. Using Lemma 1.6 we bound $\mathrm{h}(\gamma_{n+1})$ by c_2h with

$$c_2=2\log\mathrm{L}(F)+2\sum_{j=1}^{n}\deg_{X_j}F.$$

By assumption, for sufficiently large D and h, we have

$$\max_{1\le i\le n+1}|\theta_i-\gamma_i|\ge\exp\bigl\{-\varphi(dD,c_2h)\bigr\}.$$

Hence

$$\max_{1\le i\le n}|\theta_i-\gamma_i|\ge c_5^{-1}\exp\bigl\{-\varphi(dD,c_2h)\bigr\},$$

which gives the desired estimate with $c_1=d$ and $c_0=\log c_5$. □

d) Large transcendence degrees

In the present paper we consider only "small transcendence degrees". However we are tempted to propose the following conjecture.

Conjecture 1.7. – *Let $a \geq 1$, $b \geq 1$ be real numbers and $\theta_1, \ldots, \theta_n$ be complex numbers. Denote by t the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\theta_1, \ldots, \theta_n)$. Let φ be a simultaneous approximation measure for these n numbers. Let $(D_\nu)_{\nu\geq 1}$ be a non-decreasing sequence of positive integers and $(h_\nu)_{\nu\geq 1}$ be a non-decreasing sequence of positive real numbers with $D_\nu + h_\nu \to \infty$. Assume*

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

Then

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

According to Proposition 1.3, it would be sufficient to establish this result under the assumption that $\theta_1, \ldots, \theta_n$ are algebraically independent (that is $n = t$).

§2.Usual exponential function in a single variable

a) The numbers a^{β^j}

In 1949 Gel'fond (see [11], chap. III, § 4) established the algebraic independence of the two numbers α^β and α^{β^2} when α is a nonzero algebraic number (with a determination $\log\alpha \neq 0$ of its logarithm, giving rise to $\alpha^\beta = \exp(\beta\log\alpha)$), and β is a cubic irrational algebraic number. Here, we deduce this algebraic independence result from a simultaneous approximation estimate for the two numbers α^β and α^{β^2}. Like Gel'fond, we consider the more general situation where β is algebraic of degree $d \geq 2$.

Theorem 2.1. – *Let a be a nonzero complex number and β an algebraic number of degree $d \geq 2$. Choose a nonzero determination $\log a$ for the logarithm of a. There exists a positive constant C such that*

$$CD^{(d+1)/(d-1)} h^{d/(d-1)} \big(\log D + \log h\big)^{-1/(d-1)}$$

is a simultaneous approximation measure for $a, a^\beta, \ldots, a^{\beta^{d-1}}$.

Notice that for each $h \geq h_0$, there exists a positive constant $C(h)$ such that this approximation measure is bounded by $C(h)D^{(d+1)/(d-1)}(\log D)^{-1/(d-1)}$. If $d \geq 3$, this function is $o(D^2)$. From Corollary 1.2 we deduce:

Corollary 2.2. – *Let a be a nonzero complex number, $\log a$ a nonzero determination of its logarithm and β an algebraic number of degree $d \geq 3$. Then at least two of the d numbers $a, a^\beta, a^{\beta^2}, \ldots, a^{\beta^{d-1}}$ are algebraically independent. In particular, if a is algebraic and β is cubic irrational, then the two numbers a^β and a^{β^2} are algebraically independent.*

For $d = 2$ and $a = \alpha$ algebraic, Theorem 2.1 gives the following approximation measure for α^β when β is a quadratic irrational number:

$$CD^3 h^2 \big(\log D + \log h\big)^{-1}.$$

b) An effective version of the six exponentials theorem

The *six exponentials theorem*, due to Lang and Ramachandra (see for instance [1], Theorem 12.3, or [28], Cor. 2.2.3) states that

> *if $x_1, \ldots, x_d$ are $\mathbb{Q}$-linearly independent and $y_1, \ldots, y_\ell$ are also $\mathbb{Q}$-linearly independent, with $d\ell > d+\ell$, then at least one of the $d\ell$ numbers $\exp(x_i y_j)$, $(1 \le i \le d,\ 1 \le j \le \ell)$ is transcendental.*

We give a simultaneous approximation measure for these $d\ell$ numbers, assuming an extra "technical hypothesis". Next we show that such a hypothesis cannot be omitted.

Definition. Let n be a positive integer, ν a positive real number and $x_1, \ldots, x_n$ complex numbers. We say that $x_1, \ldots, x_n$ *satisfy a measure of linear independence with exponent* ν if there exists a positive integer T_0 satisfying the following property: for any n-tuple $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ and any real number $T \ge T_0$ with

$$0 < \max\{|t_1|, \ldots, |t_n|\} \le T,$$

we have

$$|t_1 x_1 + \cdots + t_n x_n| \ge \exp(-T^\nu).$$

According to this definition, if the numbers $x_1, \ldots, x_n$ satisfy a measure of linear independence, then they are linearly independent over $\mathbb{Q}$.

Theorem 2.3. – *Let d and ℓ be positive integers satisfying $d\ell > d+\ell$. Set*

$$\kappa = \frac{d\ell}{d\ell - d - \ell}\ .$$

Let $x_1, \ldots, x_d$ be complex numbers which satisfy a measure of linear independence with exponent $1/(3d)$, and also let $y_1, \ldots, y_\ell$ be complex numbers which satisfy a measure of linear independence with exponent $1/(3\ell)$. Then, there exists a positive constant C such that

$$C(Dh)^\kappa \bigl(\log D + \log h\bigr)^{1-\kappa}$$

is a simultaneous approximation measure for the $d\ell$ numbers $e^{x_i y_j}$, $(1 \le i \le d,\ 1 \le j \le \ell)$.

Remark. Earlier estimates of this type were known ([22], [23], [16]), but with a weaker dependence on D. Because of that, they are not sufficient to prove results of algebraic independence.

Assuming $d\ell \ge 2(d+\ell)$, for fixed h the simultaneous approximation measure is bounded by $o(D^2)$. Therefore, in this case, at least two of the $d\ell$ numbers $\exp(x_i y_j)$,

$(1 \le i \le d,\ 1 \le j \le \ell)$ are algebraically independent. We remark that this algebraic independence result is known, given only that $x_1, \ldots, x_d$ on one side, $y_1, \ldots, y_\ell$ on the other, are linearly independent over $\mathbb{Q}$. Here we need to add technical hypotheses (measures of linear independence). In fact, these conditions are similar to those which occur in the known results for large transcendence degrees [6], [31](see also the comment after the proof of Theorem 2.4). However, for small transcendence degrees, these extra conditions (which Gel'fond needed in his original work – cf. [11], Chap. III, § 4, Theorems I, II and III), have been shown to be unnecessary by Tijdeman [24] (see also [28], Chap. 7). The underlying method of the present work also enables us to avoid these assumptions for small transcendence degrees [21]. But in order to do so, we need to bypass Theorem 2.3.

The proof of Theorem 2.3 relies on the following statement which does not require a diophantine hypothesis.

Denote by $\mathrm{Im}(z)$ the imaginary part of a complex number z.

Theorem 2.4. – *Let d, ℓ and κ be as in Theorem 2.3. There exists a positive constant C which satisfies the following property. Let λ_{ij}, $(1 \le i \le d,\ 1 \le j \le \ell)$ be complex numbers whose exponentials $\gamma_{ij} = e^{\lambda_{ij}}$ are algebraic. Assume that the d numbers $\lambda_{11}, \ldots, \lambda_{d1}$ are linearly independent over $\mathbb{Q}$, and also that the ℓ numbers $\lambda_{11}, \ldots, \lambda_{1\ell}$ are linearly independent over $\mathbb{Q}$. Let D be the degree of the number field generated over $\mathbb{Q}$ by the $d\ell$ numbers γ_{ij}, $(1 \le i \le d,\ 1 \le j \le \ell)$, and let $h \ge 3$, $E \ge e$, $F \ge 1$ be real numbers satisfying*

$$\max_{\substack{1\le i\le d\\ 1\le j\le \ell}} \mathrm{h}(\gamma_{ij}) \le h, \qquad \max_{\substack{1\le i\le d\\ 1\le j\le \ell}} |\lambda_{ij}| \le Dh/E \quad \textit{and} \quad F = 1 + \max_{\substack{1\le i\le d\\ 1\le j\le \ell}} |\mathrm{Im}(\lambda_{ij})|.$$

Then, we have

$$\max_{\substack{1\le i\le d\\ 1\le j\le \ell}} \bigl|\lambda_{ij}\lambda_{11} - \lambda_{i1}\lambda_{1j}\bigr| \ge \exp\bigl\{-C(Dh)^\kappa (\log E)^{1-\kappa} F^{\kappa/m}\bigr\},$$

where $m = \max\{d, \ell\} - 1$.

The conclusion is a lower bound for at least one of the 2×2 minors of the matrix $\bigl(\lambda_{ij}\bigr)_{1\le i\le d, 1\le j\le \ell}$. Extensions of this result to minors of larger size can also be produced – the corresponding algebraic independence statements are given in [21].

Remark. One can prove variants of Theorems 2.3 and 2.4 which contain Gel'fond's algebraic independence results concerning the numbers x_i, $e^{x_i y_j}$, (resp. x_i, y_j, $e^{x_i y_j}$) – see [11], Chap. III, § 4, Theorems I, II and III. More generally, one can prove simultaneous approximation measures which contain the results of algebraic independence obtained by Chudnovski using Baker's method in chapter 3 of [6]. By the way, it is necessary to add the assumption $r_2 > 0$ in Theorem 3.1, p.136 of [6]: it was not known at that time that the two numbers π and e^π are algebraically independent; and it is still unknown that, for β a quadratic irrational number and λ a nonzero logarithm of an algebraic number, the two numbers λ and $e^{\beta\lambda}$ are algebraically independent.

c) Liouville numbers

We show that the conclusion of Theorem 2.3 may fail if we omit the hypotheses concerning measures of linear independence.

Let ϕ be a strictly increasing function $\mathbb{N} \to \mathbb{N}$ and let $(u_n)_{n\geq 0}$ be a bounded sequence of rational integers: $|u_n| \leq c_1$ for all $n \geq 0$. Assume $u_n \neq 0$ for an infinite set of n (hence $c_1 \geq 1$). Consider the number

$$\xi = \sum_{n\geq 0} \frac{u_n}{2^{\phi(n)}}.$$

For $N \geq 0$, define

$$q_N = 2^{\phi(N)}, \qquad p_N = \sum_{n=0}^{N} u_n 2^{\phi(N)-\phi(n)}.$$

Then $(p_N, q_N) \in \mathbb{Z}^2$, $q_N > 0$ and

$$\left|\xi - \frac{p_N}{q_N}\right| = \left|\sum_{n>N} u_n 2^{-\phi(n)}\right| \leq c_1 \sum_{n\geq N+1} 2^{-\phi(N+1)-n+N+1} \leq \frac{2c_1}{2^{\phi(N+1)}}.$$

From the upper bound

$$|e^a - e^b| \leq |a-b| \max\{e^a, e^b\} \qquad \text{for real numbers } a \text{ and } b,$$

we deduce

$$\left|2^\xi - 2^{p_N/q_N}\right| < \frac{c_2}{2^{\phi(N+1)}}$$

with a constant $c_2 = 2^{1+2c_1}c_1$ independent of N. For $a/b \in \mathbb{Q}$, we have $\mathrm{h}(2^{a/b}) = (a/b)\log 2$, hence the absolute logarithmic height of the algebraic number $2^{p_N/q_N}$ is bounded independently of N by

$$\mathrm{h}(2^{p_N/q_N}) \leq 2c_1 \log 2,$$

while its degree is $\leq q_N$.

Let d be a positive integer. Define d sequences $\big(u_{in}^{(d)}\big)_{n\geq 0}$, $(1 \leq i \leq d)$ by

$$u_{in}^{(d)} = \begin{cases} 1 & \text{if } n \equiv i \pmod{d}, \\ 0 & \text{otherwise,} \end{cases} \qquad (1 \leq i \leq d)$$

and set

$$\xi_{id} = \sum_{n\geq 1} \frac{u_{in}^{(d)}}{2^{\phi(n)}} = \sum_{q\geq 0} \frac{1}{2^{\phi(qd+i)}}, \qquad (1 \leq i \leq d).$$

Define, for $N \geq 1$,

$$p_{iN}^{(d)} = \sum_{n=1}^{N} u_{in}^{(d)} 2^{\phi(N)-\phi(n)}.$$

We get

$$\max_{1\leq i\leq d} \left| \xi_{id} - \frac{p_{iN}^{(d)}}{q_N} \right| < \frac{2}{2^{\phi(N+1)}}.$$

Moreover, assume $\phi(n+1)-\phi(n) \to \infty$ as $n \to \infty$. Then, for any tuple $(t_1,\ldots,t_d)$ of rational integers, not all of which are zero, the number $t_1\xi_{1d}+\cdots+t_d\xi_{dd}$ has a lacunary 2-adic expansion. Hence it is irrational, and therefore does not vanish (in fact if the function ϕ grows sufficiently fast, this number is transcendental). It follows that the numbers $\xi_{1d},\ldots,\xi_{dd}$ are linearly independent over $\mathbb{Q}$.

Define $x_1,\ldots,x_d$ by $x_i = \xi_{id}$, $(1 \leq i \leq d)$ and define $y_1,\ldots,y_\ell$ by $y_j = \xi_{j\ell}\log 2$ for $1 \leq j \leq \ell$. The transcendence degree t over $\mathbb{Q}$ of the field generated by the $d\ell$ numbers $e^{x_iy_j}$ satisfies $t \geq 1$ provided $d\ell > d+\ell$ and satisfies $t \geq 2$ provided $d\ell \geq 2(d+\ell)$ (cf. [4] and [28], Chap. 7). Define further $a_{iN} = p_{iN}^{(d)}$, $b_{jN} = p_{jN}^{(\ell)}$ and $\gamma_{ij} = 2^{a_{iN}b_{jN}/q_N^2}$. We get

$$\max_{1\leq i\leq d} \left| x_i - \frac{a_{iN}}{q_N} \right| \leq \frac{2}{2^{\phi(N+1)}}, \qquad \max_{1\leq j\leq \ell} \left| y_j - \frac{b_{jN}}{q_N}\log 2 \right| \leq \frac{2\log 2}{2^{\phi(N+1)}}$$

and

$$\max_{\substack{1\leq i\leq d\\ 1\leq j\leq \ell}} |e^{x_iy_j} - \gamma_{ij}| \leq \frac{8\log 2}{2^{\phi(N+1)}}.$$

The absolute logarithmic height of the numbers γ_{ij} is bounded independently of N:

$$\mathrm{h}(\gamma_{ij}) \leq \log 2.$$

The field generated over $\mathbb{Q}$ by the $d\ell$ numbers γ_{ij} has degree $\leq q_N^{2d\ell} = 4^{d\ell\phi(N)}$ over $\mathbb{Q}$. If $\varphi(D,h)$ is a simultaneous approximation measure for the $d\ell$ numbers $e^{x_iy_j}$, then for any $h \geq \max\{h_0, \log 2\}$ and any $D \geq \max\{D_0, 4^{d\ell\phi(N)}\}$, we have

$$\varphi(D,h) \geq \phi(N+1)\log 2 - 2.$$

We can choose for ϕ a function such that

$$\limsup_{N\to\infty} \frac{\phi(N+1)}{2^{4d\ell\phi(N)}} = \infty.$$

In this case $\limsup_{N\to\infty} D^{-2}\varphi(D,h) = \infty$, hence the hypothesis of Corollary 1.2 is not satisfied. Therefore we cannot deduce from Corollary 1.2 the algebraic independence of at least two of these numbers.

The argument used for lifting the obstructing subgroup in [21] shows that the underlying method to the present work yields not only simultaneous approximation measures, but also results of algebraic independence without technical hypothesis.

Remark. Consider the number
$$\theta = \sum_{n\geq 0} \frac{1}{2^{\phi(n)}},$$
where $\phi\colon \mathbb{N} \to \mathbb{N}$ is a strictly increasing function, such that
$$\phi(n+1) \geq n^2\phi(n)$$
for all $n \geq 0$. Define two sequences $(D_\nu)_{\nu\geq 1}$ and $(h_\nu)_{\nu\geq 1}$ by
$$D_\nu = \nu \quad \text{and} \quad h_\nu = \nu^{-1/2}\phi(\nu) \quad (\nu \geq 1).$$
Then $D_\nu + h_\nu \to \infty$ for $\nu \to \infty$. However, *for any positive real number C and for any sufficiently large ν, there is no algebraic number γ of degree $\leq D_\nu$ and height $\leq h_\nu$ which satisfies*
$$|\theta - \gamma| \leq \exp\{-CD_\nu^2 h_\nu\}.$$
We prove this claim by contradiction. Assume such a γ exists for some value of ν with $\nu \geq \max\{16, 2C^{-2}\}$. We compare γ to the rational number
$$\alpha = \sum_{n=1}^{\nu} \frac{1}{2^{\phi(n)}}.$$
Since $h(\alpha) = \phi(\nu)\log 2 > h_\nu$, we have $\gamma \neq \alpha$. From Liouville's inequality we deduce
$$\log|\gamma - \alpha| \geq -D_\nu(\log 2 + \phi(\nu)\log 2 + h_\nu) \geq -\nu\phi(\nu).$$
This is not possible, according to the following computation:
$$\begin{aligned}\log|\gamma - \alpha| &\leq \log 2 + \log\max\{|\theta - \gamma|, |\theta - \alpha|\}\\ &\leq \log 2 + \max\{-C\nu^{3/2}\phi(\nu), -\phi(\nu+1)\log 2 + \log 2\}\\ &< -\nu\phi(\nu).\end{aligned}$$
This example shows that the condition $h_{\nu+1} \leq bh_\nu$ in conjecture 1.7 cannot be omitted.

d) Schanuel's conjecture

Let $x_1, \ldots, x_n$ be $\mathbb{Q}$-linearly independent complex numbers. Schanuel's conjecture (see [13], Chap. 3, Historical Note) states that the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})$ is $\geq n$. Here we produce a simultaneous approximation measure for the $2n$ numbers $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$. If we select $x_i = \xi_{in}$, $(1 \leq i \leq n)$, with the previously defined numbers ξ_{in}, we see that the hypothesis of linear independence for the numbers x_i is not sufficient to get any estimate at all. This is why we assume a measure of linear independence.

Theorem 2.5. – *Let $x_1, \ldots, x_n$ be complex numbers which satisfy a measure of linear independence with exponent $2n+1$. There exists a positive constant $C = C(n)$ such that the function*

$$CD^{2+1/n}h(h+\log D)(\log h+\log D)^{-1}$$

is a simultaneous approximation measure for the $2n$ numbers $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$.

We shall also prove a variant of this statement, where no technical hypothesis is needed: we produce a lower bound for

$$\sum_{i=1}^{n} |\beta_i - \log \alpha_i|$$

when $\log \alpha_1, \ldots, \log \alpha_n$ are logarithms of algebraic numbers, while $\beta_1, \ldots, \beta_n$ are $\mathbb{Q}$-linearly independent algebraic numbers (see Theorem 8.1 below).

e) Lindemann-Weierstraß theorem

Chudnovsky [7] has shown how to prove the Lindemann–Weierstraß theorem on the algebraic independence of the numbers $e^{\beta_1}, \ldots, e^{\beta_n}$ by means of Gel'fond's method. Here is a simultaneous approximation measure for these numbers.

Theorem 2.6. – *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 the function*

$$CD^{1+(1/n)}h(\log h + D\log D)(\log h + \log D)^{-1}$$

is a simultaneous approximation measure for the numbers $e^{\beta_1}, \ldots, e^{\beta_n}$.

The estimate is not sharp enough to apply Corollary 1.2 to the numbers $\theta_i = e^{\beta_i}$, $(1 \le i \le n)$. However the function

$$\varphi(D,h) = CD^{1+(1/n)}h(\log h + D\log D)(\log h + \log D)^{-1}$$

satisfies, for $n \ge 2$,

$$\limsup_{D\to\infty} \frac{1}{D^{1+1/(n-1)}} \limsup_{h\to\infty} \frac{1}{h}\varphi(D,h) = 0.$$

Therefore conjecture 1.7 would enable us to deduce the Lindemann-Weierstrass theorem from Theorem 2.6.

f) Other examples

Theorem 2.5 contains many results of simultaneous approximation. In certain cases the estimate can be refined. Here is a first example.

Theorem 2.7. – *Let β be an irrational quadratic number and let λ be a nonzero logarithm of an algebraic number. There exists a positive constant $C = C(\beta, \lambda)$ such that*

$$CD^2 h(h + \log D)^{1/2} (\log h + \log D)^{-1/2}$$

is a simultaneous approximation measure for the two numbers λ and $e^{\beta\lambda}$.

If we choose $\lambda = 2i\pi$ and $\beta = i$, we deduce the existence of a positive absolute constant C such that

$$CD^2 h(h + \log D)^{1/2} (\log h + \log D)^{-1/2}$$

is a simultaneous approximation measure for π and e^{π}. This is so far the best known estimate, but it is not sharp enough to yield the algebraic independence of the two numbers π and e^{π}. We come back to this question in section 4.

As far as the two numbers e and π are concerned, we do not know anything better than the above mentioned individual approximation measures for e and for π, due to Fel'dman – also, we do not know anything better than Theorem 2.7 concerning a simultaneous approximation measure for the three numbers e, π and e^{π}.

The measure of simultaneous approximation for the numbers $\log\alpha_1, \ldots, \log\alpha_n$ due to Fel'dman (cf. section 1) is not sufficient to settle the open problem of the existence of two algebraically independent logarithms of algebraic numbers. However we can improve Fel'dman's measure for large D by adding a hypothesis.

Theorem 2.8. – *Let $n \geq 2$ be an integer and $\lambda_1, \ldots, \lambda_n$ be $\mathbb{Q}$-linearly independent logarithms of algebraic numbers. Assume that there exists a nonzero homogeneous polynomial $Q \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree 2, such that $Q(\lambda_1, \ldots, \lambda_n) = 0$. Then there is a positive constant C such that the function*

$$CD^2 (h + \log D)^2 (\log D)^{-2}$$

is a simultaneous approximation measure for the numbers $\lambda_1, \ldots, \lambda_n$.

Therefore, under the assumptions of this Theorem 2.8, at least two of the numbers $\lambda_1, \ldots, \lambda_n$ are algebraically independent (cf. [20], Theorem 2, and [21]).

§3. Elliptic functions

Elliptic analogues of all results in the preceding section can be proved. The estimates are sharper in the CM case. Here is the analogue of Theorem 2.1 for elliptic functions.

Theorem 3.1. – *Let $\wp$ be a Weierstraß elliptic function with algebraic invariants g_2 and g_3, let u be a complex number and let β be an algebraic number. Assume that none of the numbers $u, \beta u, \ldots, \beta^{d-1}u$ is a pole of $\wp$. There exists a positive constant C with the following property:*
a) if β is of degree $d \geq 3$ over $\mathbb{Q}$, the function

$$CD^{(d+1)/(d-2)}h^{d/(d-2)}\bigl(\log D + \log h\bigr)^{-2/(d-2)}$$

is a simultaneous approximation measure for the d numbers $\wp(\beta^i u)$, $(0 \leq i \leq d-1)$.
b) If the elliptic curve $\mathbb{E}$ associated with $\wp$ has complex multiplication, and if β is of degree $d \geq 2$ over the field of endomorphisms of $\mathbb{E}$, the function

$$CD^{(d+1)/(d-1)}h^{d/(d-1)}\bigl(\log D + \log h\bigr)^{-1/(d-1)}$$

is a simultaneous approximation measure for the d numbers $\wp(u), \wp(\beta u), \ldots, \wp(\beta^{d-1}u)$.

The assumption that *none of the numbers $u, \beta u, \ldots, \beta^{d-1}u$ is a pole of $\wp$* is not a serious restriction: if for instance u is pole of $\wp$, we deduce a simultaneous approximation measure for the remaining $d-1$ numbers $\wp(\beta u), \ldots, \wp(\beta^{d-1}u)$ by applying the theorem with u replaced by u/n, where n is a sufficiently large integer.

In the CM case, the estimate is the same as in the exponential case. In fact we shall give a single proof for the two statements (Theorem 2.1 and Theorem 3.1). From Theorem 3.1 we deduce the algebraic independence of at least two of the numbers $\wp(\beta^i u)$, $(0 \leq i \leq d-1)$, provided β is of degree ≥ 5 over $\mathbb{Q}$ in the general case, and provided β is of degree ≥ 3 over the field of endomorphisms in the CM case. In particular, in the CM case, we deduce the algebraic independence of the two numbers $\wp(\beta u)$ and $\wp(\beta^2 u)$ when $\wp(u)$ is an algebraic number and β a cubic irrational number. These algebraic independence results are due to Masser and Wüstholz [14].

In the same way we can produce other diophantine approximation estimates which yield algebraic independence results. Elliptic analogues of Theorems 2.3 and 2.4 can be proved, as well as simultaneous approximation measures related to results by G.V. Chudnovsky ([6], [7]) and R. Tubbs ([25], [26]).

§4. Gamma function

Our last theorem deals with periods of elliptic integrals of first or second kind.

Theorem 4.1. – *Let $\wp$ be a Weierstraß elliptic function with algebraic invariants g_2 and g_3. Denote by (ω_1, ω_2) a fundamental pair of periods of $\wp$, and by η_1, η_2 the corresponding quasi-periods of the Weierstraß zeta function associated with $\wp$:*

$$\zeta' = -\wp, \qquad \zeta(z+\omega_i) = \zeta(z) + \eta_i, \quad (i = 1, 2).$$

There exists a positive constant C such that

$$CD^{3/2}(h+\log D)^{3/2}$$

is a simultaneous approximation measure for the four numbers $\omega_1, \omega_2, \eta_1, \eta_2$.

We deduce a well known result due to Chudnovsky [6] (Chap. 1, § 2, Theorem 1): *the field $\mathbb{Q}(\omega_1, \omega_2, \eta_1, \eta_2)$ has transcendence degree ≥ 2 over $\mathbb{Q}$.* In the CM case, the transcendence degree is 2.

Theorem 4.1 shows that there exists an absolute positive constant C satisfying the following property: *let γ_1 and γ_2 be algebraic numbers. Define*

$$h = \max\{3, \mathrm{h}(\gamma_1), \mathrm{h}(\gamma_2)\} \quad \textit{and} \quad D = [\mathbb{Q}(\gamma_1, \gamma_2) : \mathbb{Q}].$$

Then

$$|\Gamma(1/4) - \gamma_1| + |\pi - \gamma_2| \geq \exp\{-CD^{3/2}(h+\log D)^{3/2}\}.$$

It follows that *the two numbers $\Gamma(1/4)$ and π are algebraically independent* (cf. [6], Chap. 7, § 1, Cor. 1.7).

Remarks.

1. One can prove a more general statement than Theorem 4.1 which deals with the universal extension of an abelian variety of dimension g by $\mathbb{G}_{\mathrm{a}}^g$. The corresponding result of algebraic independence is stated by Chudnovsky in [6], Introduction, Theorem 9, p.9.

2. Very recently, dramatic progress has been achieved on this topic. The story started with the solution by K. Barré-Sirieix, G. Diaz, F. Gramain and G. Philibert [2] of a conjecture of Mahler (in the complex case) and Manin (in the p-adic case) on the transcendence of the values of the modular function $J(q)$ for algebraic q with $0 < |q| < 1$. This work gave the impetus to Nesterenko's proof of the algebraic independence of the three numbers π, e^π and $\Gamma(1/4)$ (see [17]). At the same time, Nesterenko produces diophantine approximation results, including a measure of algebraic independence. A slightly different approach is used by Philippon [19] who also produces diophantine estimates, including a simultaneous approximation measure for these three numbers: *for any $\epsilon > 0$ there exists a positive constant $C(\epsilon)$ such that the function*

$$C(\epsilon)(Dh)^{(4/3)+\epsilon}$$

is a simultaneous approximation measure for the three numbers π, e^π and $\Gamma(1/4)$.

Conjecture 1.7 suggests that such a measure for three numbers with an exponent $< 3/2$ can take place only when these numbers are algebraically independent. On the other hand this estimate does not include the simultaneous approximation measure for π and e^π which we have deduced from Theorem 2.7, nor the simultaneous approximation measure for π and $\Gamma(1/4)$ which follows from Theorem 4.1.

§5. A special case of the explicit algebraic subgroup theorem

The main tool in the proof of each of the above results is Theorem 2.1 of [33]. This theorem provides an explicit version of the algebraic subgroup theorem, in the context of an arbitrary commutative algebraic group. For the convenience of the reader, we prove here a special case of this theorem that is sufficient for the proof of all our results, with the exception of Theorem 4.1. The proof of the latter, given in §11, relies directly on Theorem 2.1 of [33]. We try to conform, as much as possible, with the notations of [33].

Let d_0, d_1 and d_2 be integers ≥ 0 whose sum d is positive, let $K \subset \mathbb{C}$ be a number field, let D be its degree over $\mathbb{Q}$, and let $\mathbb{E} \subset \mathbb{P}_2$ be an elliptic curve defined by a Weierstraß equation

$$\mathbb{E} \,:\, X_0X_2^2 - 4X_1^3 + g_2X_0^2X_1 + g_3X_0^3 = 0 \tag{5.1}$$

with $g_2, g_3 \in K$. Put $G_0 = \mathbb{G}_{\rm a}^{d_0}$ and $n = d_1 + d_2$. We embed G_0 in $\mathbb{P}_{d_0}$ and $\mathbb{G}_{\rm m}$ in $\mathbb{P}_1$ in such a way that their exponential maps be given respectively by

$$\exp_{G_0}(z_1, \ldots, z_{d_0}) = (1 : z_1 : \cdots : z_{d_0}) \quad \text{and} \quad \exp_{\mathbb{G}_{\rm m}}(z) = (1 : e^z).$$

We also denote by $\wp$ the Weierstraß $\wp$-function attached to $\mathbb{E}$, so that the exponential map of $\mathbb{E}$, from $\mathbb{C}$ to $\mathbb{E}(\mathbb{C})$, is given, away from the poles of $\wp$, by

$$\exp_{\mathbb{E}}(z) = \big(1 : \wp(z) : \wp'(z)\big).$$

The product

$$G = G_0 \times \mathbb{G}_{\rm m}^{d_1} \times \mathbb{E}^{d_2}$$

therefore embeds into $\mathbb{P}_{d_0} \times (\mathbb{P}_1)^{d_1} \times (\mathbb{P}_2)^{d_2}$. Its exponential map

$$\exp_G \,:\, T_G(\mathbb{C}) = \mathbb{C}^d \longrightarrow G(\mathbb{C})$$

is given by the product of the exponential maps of its factors. For simplicity however, we often identify $G_0(\mathbb{C})$ with the additive group $\mathbb{C}^{d_0}$ and $\mathbb{G}_{\rm m}(\mathbb{C})$ with the multiplicative group $\mathbb{C}^\times$.

Given an algebraic subset V of G, we denote by $\mathcal{H}(V\,; T_0, T_1, \ldots, T_n)$ the product by $(\dim V)!$ of the homogeneous part of degree $\dim V$ of its Hilbert-Samuel polynomial (with respect to the above embedding of G). Given a finitely generated subgroup Γ of $G(K)$, a finite set of generators $\gamma_1, \ldots, \gamma_\ell$ of Γ, and positive integers $S_1, \ldots, S_\ell$, we denote by $\Gamma(S_1, \ldots, S_\ell)$ the set of all elements of Γ of the form $s_1\gamma_1 + \cdots + s_\ell\gamma_\ell$ with integral coefficients s_j satisfying $0 \leq s_j < S_j$ for $j = 1, \ldots, \ell$. When $S_1 = \ldots = S_\ell = S$, we simply denote this set by $\Gamma(S)$. Similarly, if Y is a subgroup of $\mathbb{C}^d$ generated by a given finite set of points $\eta_1, \dots, \eta_\ell$, we define $Y(S_1, \dots, S_\ell)$ as the set of all linear combinations of these points with integral coefficients in the same range. Finally, we denote by $|\mathbf{z}|$ the supremum norm of a point $\mathbf{z}$ of $\mathbb{C}^d$:

$$|(z_1, \dots, z_d)| = \max_{1 \le i \le d} |z_i|.$$

This definition applies in particular to elements of $\mathbb{Z}^d$.

For $w = (\alpha_1, \dots, \alpha_d) \in K^d$, we denote by $h(1 : w)$ the absolute logarithmic height of the projective point $(1 : \alpha_1 : \cdots : \alpha_d)$.

Theorem 5.1. *There exist positive constants $C_1 = C_1(d) \ge e$ and $C_2 = C_2(d, \ell, \mathbb{E})$ with the following property. Let ℓ_0 and ℓ_1 be integers ≥ 0, let $w'_1, \dots, w'_{\ell_0}$ and $\eta'_1, \dots, \eta'_{\ell_1}$ be elements of $\mathbb{C}^d$, let $w_1, \dots, w_{\ell_0}$ be elements of K^d, and let $\eta_1, \dots, \eta_{\ell_1}$ be elements of $\mathbb{C}^d$ whose images $\gamma_1, \dots, \gamma_{\ell_1}$ under $\exp_G$ all belong to $G(K)$. Denote by r the dimension of the subspace of $\mathbb{C}^d$ generated by $w'_1, \dots, w'_{\ell_0}$ and $\eta'_1, \dots, \eta'_{\ell_1}$. Denote by W the subspace of K^d generated by $w_1, \dots, w_{\ell_0}$, and denote by Γ the subgroup of $G(K)$ generated by $\gamma_1, \dots, \gamma_{\ell_1}$. Assume that $\eta'_1, \dots, \eta'_{\ell_1}$ do not all belong to $\mathbb{C}^{d_0} \times \{0\}^n$. Suppose that we are given real numbers $A_1, \dots, A_n \ge e^2$, $B_1, B_2 \ge 2d$ and $E \ge e$, integers $S_0, S_1, \dots, S_{\ell_1} \ge 1$ and $T_0, T_1, \dots, T_n \ge 1$, and real numbers $U, V > 0$. Suppose $B_2 \ge C_2$ if $d_2 > 0$. Write*

$$\eta_j = (\beta_{1,\ell_0+j}, \dots, \beta_{d_0,\ell_0+j}\,,\, u_{1j}, \dots, u_{nj})$$

for $j = 1, \dots, \ell_1$, and suppose

$$\log\Big(\sum_{j=1}^{\ell_1} S_j\Big) + \sum_{j=1}^{\ell_1} h(\beta_{i,\ell_0+j}) \le \log B_1, \qquad (1 \le i \le d_0),$$

$$h(1 : w_j) \le \log B_2, \qquad (1 \le j \le \ell_0),$$

$$\max\Big\{\sum_{j=1}^{\ell_1} S_j h(e^{u_{ij}}),\ \frac{E}{D}\sum_{j=1}^{\ell_1} S_j |u_{ij}|\Big\} \le \log A_i, \qquad (1 \le i \le d_1),$$

$$C_2 \max_{1 \le j \le \ell_1} \Big\{S_j^2\Big(h\big(\wp(u_{ij})\big) + 1\Big),\ \frac{E^2}{D} S_j^2 |u_{ij}|^2\Big\} \le \log A_i, \qquad (d_1 < i \le n).$$

Suppose also

$$|w'_j - w_j| \le e^{-2V} \quad (1 \le j \le \ell_0) \quad \textit{and} \quad |\eta'_j - \eta_j| \le e^{-2V} \quad (1 \le j \le \ell_1),$$

and that the parameters satisfy

$$D \log B_1 \ge \log E, \quad D \log B_2 \ge \log E, \quad B_2 \ge dS_0 + T_0 + T_1 + \cdots + T_n, \tag{5.2}$$

$$DT_0 \log B_1 \le U, \quad DS_0 \log B_2 \le U, \quad \sum_{i=1}^{n} DT_i \log A_i \le U, \quad C_1 U \le V \tag{5.3}$$

and the main condition

$$\frac{1}{8\cdot 3^{d_2}}\exp\Big(\frac{U}{2D}\Big) > \binom{T_0+d_0}{d_0}(T_1+1)\cdots(T_n+1) \geq 4\Big(\frac{V}{\log E}\Big)^r. \tag{5.4}$$

Then, there exists a connected algebraic subgroup G^* of G, distinct from G, incompletely defined in G by polynomials of multidegree

$$\leq (T_0, T_1, \dots, T_{d_1}, 2T_{d_1+1}, \dots, 2T_n),$$

such that, if we put

$$\ell_0^* = \dim_K\big((W + T_{G^*}(K))/T_{G^*}(K)\big),$$

we obtain

$$S_0^{\ell_0^*}\,\mathrm{Card}\left(\frac{\Gamma(S_1,\dots,S_{\ell_1}) + G^*(K)}{G^*(K)}\right)\cdot \mathcal{H}(G^*\,;\,T_0,T_1,\dots,T_n) \leq \frac{6^{d_2}d!}{d_0!}T_0^{d_0}T_1\cdots T_n.$$

Proof. Let $M = S_1\cdots S_{\ell_1}$, and let $\mathcal{S}$ be the set of all points $\mathbf{s} = (s_1,\dots,s_{\ell_1}) \in \mathbb{Z}^{\ell_1}$ with $0 \leq s_j < S_j$, $(1 \leq j \leq \ell_1)$. Choose an enumeration $\mathbf{s}_1,\dots,\mathbf{s}_M$ of $\mathcal{S}$ in such a way that, if $\mathbf{s}_k = (s_{1k},\dots,s_{\ell_1 k})$, then, for $k = 1,\dots,\ell_1$, we have

$$\eta'_k = \sum_{j=1}^{\ell_1} s_{jk}\eta'_j \quad\text{and}\quad \eta_k = \sum_{j=1}^{\ell_1} s_{jk}\eta_j.$$

Use the same formulas, to define η'_k and η_k for $k = \ell_1+1,\dots,M$, and put $\gamma_k = \exp_G(\eta_k)$ for $k = 1,\dots,M$. Then the set $\Sigma = \{\gamma_1,\dots,\gamma_M\}$ is simply $\Gamma(S_1,\dots,S_{\ell_1})$. We now show that these data and the present choice of parameters satisfy all constraints in Theorem 2.1 of [33].

We first verify the height constraints in §2 e) of [33]. For $i = 1,\dots,d_0$, the point of $\mathbb{P}_M(K)$ whose coordinates are 1 and the linear combinations $\sum_{j=1}^{\ell_1} s_j\beta_{i,\ell_0+j}$ with coefficients $(s_1,\dots,s_{\ell_1}) \in \mathcal{S}$ has height

$$\leq \log\Big(\sum_{j=1}^{\ell_1} S_j\Big) + \sum_{j=1}^{\ell_1} h(\beta_{i,\ell_0+j}) \leq \log B_1.$$

For any $i = 1,\dots,d_1$ and any $(s_1,\dots,s_{\ell_1}) \in \mathcal{S}$, we have

$$h\Big(\exp\Big(\sum_{j=1}^{\ell_1} s_j u_{ij}\Big)\Big) \leq \sum_{j=1}^{\ell_1} S_j h(e^{u_{ij}}) \leq \log A_i,$$

$$\frac{E}{D}\Big|\sum_{j=1}^{\ell_1} s_j u_{ij}\Big| \le \frac{E}{D}\sum_{j=1}^{\ell_1} S_j|u_{ij}| \le \log A_i,$$

and $2/D \le 2 \le \log A_i$. Similarly, §4 c) of [33] shows that there is a positive constant $C_3 = C_3(\mathbb{E})$ such that for any $i = d_1+1,\dots,n$ and any $(s_1,\dots,s_{\ell_1}) \in \mathcal{S}$, we have

$$\begin{aligned} h\Big(\exp_{\mathbb{E}}\Big(\sum_{j=1}^{\ell_1} s_j u_{ij}\Big)\Big) &\le \ell_1^2 C_3 \max_{1\le j\le \ell_1}\big\{S_j^2\big(h\big(\exp_{\mathbb{E}}(u_{ij})\big)+1\big)\big\} \\ &\le \ell_1^2 C_3^2 \max_{1\le j\le \ell_1}\big\{S_j^2\big(h\big(\wp(u_{ij})\big)+1\big)\big\} \\ &\le \log A_i, \end{aligned}$$

$$\frac{1}{D}H^+\Big(Ed\Big|\sum_{j=1}^{\ell_1} s_j u_{ij}\Big|+2\Big) \le C_3\frac{(d\ell_1+1)^2}{D}\max_{1\le j\le \ell_1}\max\Big\{1, E^2S_j^2|u_{ij}|^2\Big\} \le \log A_i,$$

and

$$\frac{1}{D}H^-\Big(d\Big|\sum_{j=1}^{\ell_1} s_j u_{ij}\Big|\Big) \le C_3 \le \log A_i,$$

provided $C_2 \ge \max\{\ell_1^2C_3^2, (d\ell_1+1)^2C_3\}$.

The conditions in §2 f) of [33] are fulfilled because of (5.2), (5.3) and the hypothesis $B_2 \ge C_2$ if $d_2 > 0$. Moreover, the assumption that not all of $\eta_1',\dots,\eta_M'$ belong to $\mathbb{C}^{d_0}\times\{0\}^n$ implies that the integer r_3 defined in §2 c) is positive. Therefore, since the Hilbert-Samuel function of G verifies

$$\binom{T_0+d_0}{d_0}\prod_{i=1}^n(T_i+1) \le H(G;T_0,\dots,T_n) \le 3^{d_2}\binom{T_0+d_0}{d_0}\prod_{i=1}^n(T_i+1),$$

the main constraint in §2 g) is satisfied if

$$\frac{1}{8\cdot 3^{d_2}}\exp\Big(\frac{U}{2D}\Big) > \binom{T_0+d_0}{d_0}\prod_{i=1}^n(T_i+1) \ge 4\binom{T_0+r_1}{r_1}\binom{dS_0+r_2}{r_2}\Big(\frac{V}{\log E}\Big)^{r_3}.$$

This last condition follows from (5.4) because we have $r_1+r_2+r_3 = r$,

$$\binom{T_0+r_1}{r_1} \le (2T_0)^{r_1} \le \Big(\frac{2U}{D\log B_1}\Big)^{r_1} \le \Big(\frac{V}{\log E}\Big)^{r_1},$$

and

$$\binom{dS_0+r_2}{r_2} \le \big((d+1)S_0\big)^{r_2} \le \Big(\frac{(d+1)U}{D\log B_2}\Big)^{r_2} \le \Big(\frac{V}{\log E}\Big)^{r_2},$$

provided $C_1 \ge d+1$. Finally, for any $(s_1,\dots,s_{\ell_1}) \in \mathcal{S}$, we have

$$\Big|\sum_{j=1}^{\ell_1} s_j\eta_j' - \sum_{j=1}^{\ell_1} s_j\eta_j\Big| \le \Big(\sum_{j=1}^{\ell_1} S_j\Big)e^{-2V} \le B_1e^{-2V} \le e^{-V},$$

since $B_1 \le e^U$. Thus, all the hypotheses of Theorem 2.1 of [33] are satisfied. The conclusion follows. $\square$

§6. Proofs of Theorems 2.1 and 3.1

We prove simultaneously both theorems. Let D be a positive integer, let c_0, h be positive real numbers with $h \geq c_0 \geq 3$, and let $\gamma_0, \ldots, \gamma_{d-1}$ be algebraic numbers with

$$\max\bigl\{\mathrm{h}(\gamma_0), \ldots, \mathrm{h}(\gamma_{d-1})\bigr\} \leq h \quad \text{and} \quad [\mathbb{Q}(\gamma_0, \ldots, \gamma_{d-1}) : \mathbb{Q}] \leq D.$$

In the case of Theorem 2.1, we assume

$$\max_{0 \leq i \leq d-1} |a^{\beta^i} - \gamma_i| \leq e^{-4V}$$

where

$$V^{d-1} = c_0^{9d-1} D^{d+1} h^d \bigl(\log D + \log h\bigr)^{-1}. \tag{6.1}$$

In the case of Theorem 3.1, we denote by $\mathbb{E}$ the elliptic curve associated to the function $\wp$. For part a), we assume

$$\max_{0 \leq i \leq d-1} |\wp(\beta^i u) - \gamma_i| \leq e^{-4V} \tag{6.2}$$

where

$$V^{d-2} = c_0^{9d-2} D^{d+1} h^d \bigl(\log D + \log h\bigr)^{-2}.$$

For part b), we assume that (6.2) holds with V given by (6.1). We will derive a contradiction assuming that c_0 is sufficiently large (depending only on β and $\log a$ for Theorem 2.1, on β, u and $\mathbb{E}$ for Theorem 3.1). Since V is an increasing function of D, we may assume $D = [\mathbb{Q}(\gamma_0, \ldots, \gamma_{d-1}) : \mathbb{Q}]$.

In the situation of Theorem 2.1, we put $A = \mathbb{Z}$, $k = \mathbb{Q}$, $\Omega = 2\pi\sqrt{-1}\,\mathbb{Z}$, $\varrho = 1$ and $\nu = 1$, and we apply Theorem 5.1 with the group

$$G = \mathbb{G}_{\mathrm{a}} \times G_1, \quad \text{where} \quad G_1 = \mathbb{G}_{\mathrm{m}}^d.$$

Thus, we have $d_0 = 1$, $d_1 = d$, $d_2 = 0$ and, in the notations of Theorem 5.1, d is replaced by $d+1$. We put $u = \log a$, and, for $0 \leq i \leq d-1$, we denote by u_i the determination of the logarithm of γ_i which is closest to $\beta^i u$. Then, we have

$$\max_{0 \leq i \leq d-1} |\beta^i u - u_i| \leq e^{-3V}, \qquad (0 \leq i \leq d-1). \tag{6.3}$$

In the situation of Theorem 3.1, we denote by Ω the group of periods of $\mathbb{E}$. For part a), we put $A = \mathbb{Z}$, $k = \mathbb{Q}$, $\varrho = 2$ and $\nu = 1$. For part b), we choose a non trivial endomorphism of

$\mathbb{E}$ corresponding to some imaginary quadratic number τ, and we put $A = \mathbb{Z}[\tau]$, $k = \mathbb{Q}(\tau)$, $\varrho = \nu = 2$. For both, we apply Theorem 5.1 with the group

$$G = \mathbb{G}_{\mathrm{a}} \times G_2, \quad \text{where} \quad G_2 = \mathbb{E}^d.$$

Thus, we have $d_0 = 1$, $d_1 = 0$, $d_2 = d$ and again, in the notations of Theorem 5.1, d is replaced by $d+1$. For $i = 0, \dots, d-1$, we denote by u_i the complex number which is closest to $\beta^i u$ and satisfies $\wp(u_i) = \gamma_i$. Then (6.3) holds in this case as well.

In all cases, we have $\nu = [k : \mathbb{Q}]$, $\varrho = \mathrm{rank}_{\mathbb{Z}}\, \Omega$ and $d > \varrho/\nu$. Moreover, β is algebraic over k of degree d. So, we can write

$$\beta^d = b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}, \tag{6.4}$$

with $b_0, b_1, \dots, b_{d-1} \in k$. We define recursively complex numbers $u_d, \dots, u_{2d-2}$ by the conditions

$$u_{i+d} = b_0 u_i + b_1 u_{i+1} + \cdots + b_{d-1} u_{i+d-1}, \qquad (0 \le i \le d-2).$$

We put $\ell_0 = 0$, $\ell_1 = \nu d$, and

$$\eta'_j = \bigl(\beta^{j-1}\,;\, \beta^{j-1}u, \beta^j u, \dots, \beta^{j+d-2}u\bigr), \qquad (1 \le j \le d),$$

$$\eta_j = \bigl(\beta^{j-1}\,;\, u_{j-1}, u_j, \dots, u_{j+d-2}\bigr), \qquad (1 \le j \le d).$$

If $\nu = 2$, we also define

$$\eta'_{d+j} = \tau\eta'_j \quad \text{and} \quad \eta_{d+j} = \tau\eta_j, \qquad (1 \le j \le d).$$

Thanks to (6.3) and (6.4), these points satisfy

$$|\eta'_j - \eta_j| \le e^{-2V}, \qquad (1 \le j \le \ell_1).$$

Moreover, since $\eta'_1, \dots, \eta'_{\ell_1}$ generate a subspace of $\mathbb{C}^{d+1}$ of dimension 1, we have $r = 1$. Let Γ be the subgroup of $G(\mathbb{C})$ generated by the points $\exp_G(\eta_j)$, $(1 \le j \le \ell_1)$, and let K be the smallest extension of k such that G is defined over K and $\Gamma \subset G(K)$. Then, the degree of K over $\mathbb{Q}$ satisfies

$$D \le [K : \mathbb{Q}] \le c_0 D.$$

The parameter V defined above is given in all cases by

$$V^{d-\varrho/\nu} = c_0^{9d-\varrho/\nu} D^{d+1} h^d \bigl(\log D + \log h\bigr)^{-\varrho/\nu}$$

Define $U = c_0^{-1}V$ and the remaining parameters by

$$T_0 = \left[\frac{U}{c_0^3 D(\log D + \log h)}\right], \qquad T_1 = \cdots = T_d = T = \left[\left(c_0^5 D\right)^{1/d}\right],$$

$$S_0 = 1, \qquad S_1 = \cdots = S_{\ell_1} = S = \left[\left(\frac{U}{c_0^3 DTh}\right)^{1/\varrho}\right],$$

$$A_1 = \cdots = A_d = \exp\{c_0 S^\varrho h\}, \quad B_1 = S^{c_0}, \quad B_2 = \exp\{U/(c_0 D)\}, \quad E = (Dh)^{1/\varrho}.$$

Then, S_0, S, T_0 and T are positive integers and S satisfies

$$(Dh)^{1/(d\nu)} \leq S \leq (Dh)^{c_0}.$$

Moreover, one verifies that all the conditions of Theorem 5.1 are fulfilled, and that we have

$$S^{d\nu} > 6^{d_2}(d+1)!T_0 T^d. \tag{6.5}$$

This last condition ensures that the conclusion of Theorem 5.1 is non trivial as we will now see.

Theorem 5.1 shows that there exists an algebraic subgroup $G^* = G_0^* \times G_\varrho^*$ of $G = \mathbb{G}_{\mathrm{a}} \times G_\varrho$, which is defined over K, which is also incompletely defined by equations of multidegrees $\leq (T_0, \varrho T, \ldots, \varrho T)$, with $G^* \neq G$, such that

$$\mathrm{Card}\left(\frac{\Gamma(S) + G^*(K)}{G^*(K)}\right) \leq 6^{d_2}(d+1)!T_0^{d_0^*} \times T^{d_\varrho^*},$$

where d_0^* is the codimension of G_0^* in $\mathbb{G}_{\mathrm{a}}$, while d_ϱ^* is the codimension of G_ϱ^* in G_ϱ. Note that, because of (6.5), the right hand side of this inequality is $< S^{\ell_1}$. Moreover, since $1, \beta, \ldots, \beta^{d-1}$ are linearly independent over k, the projection of $\Gamma(S)$ on the factor $\mathbb{G}_{\mathrm{a}}$ of G has cardinality S^{ℓ_1}. We deduce $G_0^* = \mathbb{G}_{\mathrm{a}}$ and $d_0^* = 0$. Let Γ_ϱ be the projection of Γ on the factor G_ϱ. For $j = 1, \ldots, \ell_1$, we denote by y_j the element of $\mathbb{C}^d$ formed by the last d coordinates of η_j. Then, the points $\exp_{G_\varrho}(y_j)$, $(1 \leq j \leq \ell_1)$, constitute a system of generators of Γ_ϱ, and we have

$$\mathrm{Card}\left(\frac{\Gamma(S) + G^*(K)}{G^*(K)}\right) = \mathrm{Card}\left(\frac{\Gamma_\varrho(S) + G_\varrho^*(K)}{G_\varrho^*(K)}\right) \geq S^{\ell_1}\,\mathrm{Card}(\mathcal{E})^{-1}$$

where $\mathcal{E}$ denotes the set of points $\mathbf{s} = (s_1, \ldots, s_{\ell_1}) \in \mathbb{Z}^{\ell_1}$ with $|\mathbf{s}| < S$ and

$$\exp_{G_\varrho}\Big(\sum_{j=1}^{\ell_1} s_j \eta_j\Big) \in G_\varrho^*(K) \tag{6.6}$$

(compare with Lemma 10.3 in [32]). This implies

$$S^{\ell_1}\,\mathrm{Card}(\mathcal{E})^{-1} \le (d+1)!6^{d_2}T^d$$

and so, by (6.5), we get $\mathrm{Card}(\mathcal{E}) \ge T_0$. Since $T_0 \ge 4S^{\varrho} > (2S-1)^{\varrho}$, this means that $\mathcal{E}$ contains at least $\varrho+1$ elements which are linearly independent over $\mathbb{Q}$. We will show that this is impossible.

Since the subgroup G^* is distinct from G and incompletely defined in G by polynomials of multidegrees $\le (T_0, \varrho T, \ldots, \varrho T)$, there exists a point $\mathbf{t} = (t_1, \ldots, t_d)$ in A^d with

$$|\mathbf{t}| \le c_0 T^{\varrho/\nu} \le c_0 T^2$$

such that G^*_{ϱ} is contained in the connected algebraic subgroup of G_{ϱ} of codimension 1 whose Lie algebra is the kernel of the linear map:

$$\begin{array}{cccc} g: & \mathbb{C}^d & \longrightarrow & \mathbb{C} \\ & (z_1, \ldots, z_d) & \mapsto & t_1 z_1 + \cdots + t_d z_d \end{array}$$

(see [32], Chap. 8 for multiplicative groups, [15], Theorem III, p. 425 for elliptic curves). For any point $(s_1, \ldots, s_{\ell_1}) \in \mathbb{Z}^{\ell_1}$ satisfying (6.6), we have

$$g\Big(\sum_{j=1}^{\ell_1} s_j y_j\Big) \in \Omega.$$

Define a mapping $f\colon \mathbb{Z}^{\ell_1} \to \mathbb{C}$ by

$$f(s_1, \ldots, s_{\ell_1}) = g\Big(\sum_{j=1}^{\ell_1} s_j y_j\Big),$$

and fix $\rho+1$ linearly independent points of $\mathcal{E}$. Since the images under f of these points are elements of Ω of norm $\le c_0^2 S T^2$, the pigeonhole principle shows that the kernel of f contains a linear combination of these points with integral coefficients which are bounded above in absolute value by

$$c_0\big(c_0^2 S T^2\big)^{\varrho} \le c_0^5 S^2 T^4,$$

and not all zero. Let $\mathbf{s} = (s_1, \ldots, s_{\ell_1}) \in \mathbb{Z}^{\ell_1}$ be such a point. The relation $f(\mathbf{s}) = 0$ gives

$$\sum_{j=1}^{d}\sum_{i=1}^{d} a_j t_i u_{j+i-2} = 0 \quad \text{where} \quad a_j = \begin{cases} s_j & \text{if } \nu = 1 \\ s_j + s_{d+j}\tau & \text{if } \nu = 2. \end{cases}$$

Since the numbers $|\beta^i u - u_i|$ are bounded from above by e^{-2V} for $i = 0, \ldots, 2d-2$, we deduce

$$\Big|\Big(\sum_{j=1}^{d} a_j \beta^{j-1}\Big)\Big(\sum_{i=1}^{d} t_i \beta^{i-1}\Big)\Big| = \Big|\sum_{j=1}^{d}\sum_{i=1}^{d} a_j t_i \beta^{j+i-2}\Big| \le e^{-V}.$$

This is impossible because, since β is of degree $d \geq 2$ over k, the above product does not vanish, and Liouville's inequality shows that it is bounded below by $\left(c_0^7 S^3 T^6\right)^{1-d\nu}$. □

Remark. A variant of this proof can be given with the group $G = G_\varrho$, using $d_0 = 0$, $\ell_0 = 1$, $\ell_1 = d\nu$,

$$w_1 = (1, \beta, \ldots, \beta^{d-1})$$

and by deleting the first coordinate of the points $\eta'_1, \ldots, \eta'_{\ell_1}$ and $\eta_1, \ldots, \eta_{\ell_1}$.

§7. Proof of Theorems 2.3 and 2.4

Proof of Theorem 2.4. Fix a constant $c_0 \geq 1$, and define

$$V = c_0^{10\kappa+1}(Dh)^\kappa (\log E)^{1-\kappa} F^{\kappa/m}.$$

We will assume

$$\max_{\substack{1\leq i\leq d \\ 1\leq j\leq \ell}} \left|\lambda_{ij}\lambda_{11} - \lambda_{i1}\lambda_{1j}\right| < e^{-3V},$$

and show that, if c_0 is sufficiently large in terms of d and ℓ, this hypothesis leads to a contradiction. This will prove the theorem with $C = 3c_0^{10\kappa+1}$. Each computation below assume that c_0 is sufficiently large as a function of d and ℓ.

By replacing the matrix (λ_{ij}) by its transpose if necessary, we may assume that $\ell \geq d$. Since $d\ell > d + \ell$, this implies $d \geq 2$ and $\ell \geq 3$, and we have $m = \ell - 1$. By permuting between themselves the columns of this matrix, we may also assume that $\gamma_{11} \neq 1$. Then, Liouville's inequality applied to $|\gamma_{11} - 1|$ gives

$$|\lambda_{11}| \geq \frac{1}{2}\min\left\{|\gamma_{11} - 1|,\, 1\right\} \geq \exp\{-D(\log 2) - Dh\} \geq \exp\{-2Dh\}.$$

Since $Dh/E \geq |\lambda_{11}|$, this implies $\log E \leq 3Dh$. So, we get $V \geq c_0^{10\kappa}Dh$, and thus

$$\max_{\substack{1\leq i\leq d \\ 1\leq j\leq \ell}} \left|(\lambda_{11}^{-1}\lambda_{1j})\lambda_{i1} - \lambda_{ij}\right| \leq |\lambda_{11}|^{-1}e^{-3V} \leq e^{-2V}.$$

Denote by K the field generated over $\mathbb{Q}$ by the $d\ell$ numbers γ_{ij}. Put $U = c_0^{-1}V$, and define T and S to be the largest integers satisfying respectively

$$T^d \leq c_0^2 \frac{U}{\log E} \quad \text{and} \quad S^\ell \leq c_0^8 \frac{U}{\log E} F^{\ell/(\ell-1)}.$$

We apply Theorem 5.1 to the algebraic group $G = \mathbb{G}_{\mathrm{m}}^d$ with the parameters $d_0 = \ell_0 = 0$, $d_1 = d$, $\ell_1 = \ell$,

$$\log A_1 = \cdots = \log A_d = c_0 Sh, \quad B_1 = B_2 = e^{U/D},$$

$$T_0 = S_0 = 1, \quad T_1 = \cdots = T_d = T, \quad S_1 = \cdots = S_\ell = S,$$

and the points

$$\eta'_j = \lambda_{11}^{-1}\lambda_{1j}(\lambda_{11}, \ldots, \lambda_{d1}) \quad \text{and} \quad \eta_j = (\lambda_{1j}, \ldots, \lambda_{dj}), \qquad (1 \le j \le \ell).$$

We have $G(K) = (K^\times)^d$, and Γ is the subgroup of $G(K)$ generated by the points

$$\gamma_j = \exp_G(\eta_j) = (\gamma_{1j}, \ldots, \gamma_{dj}), \qquad (1 \le j \le \ell).$$

Since $\eta'_1, \ldots, \eta'_\ell$ span a one-dimensional subspace of $\mathbb{C}^d$, one verifies that all the conditions of Theorem 5.1 are satisfied with $r = 1$. Thus, there exists a connected algebraic subgroup G^* of G, different from G, which is defined by equations of partial degrees $\le T$, such that

$$\mathrm{Card}\Big(\frac{\Gamma(S) + G^*(K)}{G^*(K)}\Big)\mathcal{H}(G^*\,; T, \ldots, T) \le d! T^d.$$

Let $d^* > 0$ be the codimension of G^* in G, and let Φ be the subgroup of $\mathbb{Z}^d$ consisting of all points $(t_1, \ldots, t_d) \in \mathbb{Z}^d$ for which the monomial $Y_1^{t_1} \cdots Y_d^{t_d} \in \mathbb{Z}[Y_1^{\pm 1}, \ldots, Y_d^{\pm 1}]$ induces the trivial character on G^*. Then, Φ has rank d^*, and we obtain

$$\mathcal{H}(G^*\,; T, \ldots, T) \ge c_0^{-1} \det(\Phi) T^{d-d^*}$$

where $\det \Phi$ denotes the determinant of Φ (see §3 (b) of [3]). Put

$$\mathcal{E} = \Big\{ (s_1, \ldots, s_\ell) \in \mathbb{Z}^\ell\,; \sum_{j=1}^{\ell} s_j \gamma_j \in G^*(K) \text{ and } |s_j| < S \text{ for } j = 1, \ldots, \ell \Big\}.$$

Then, we also have

$$\mathrm{Card}\Big(\frac{\Gamma(S) + G^*(K)}{G^*(K)}\Big)\,\mathrm{Card}(\mathcal{E}) \ge S^\ell$$

(see for example the remark after Lemma 10.3 in [32]). Combining the last three inequalities, we obtain

$$S^\ell \det(\Phi) \le d! c_0 T^{d^*}\,\mathrm{Card}(\mathcal{E}).$$

First, assume $d^* < d$, and let φ be a nonzero element of Φ of smallest supremum norm. By Minkowski's first convex body theorem, and Vaaler's cube slicing inequality [27], we get

$$|\varphi| \le \det(\Phi)^{1/d^*} \le \det(\Phi),$$

since Φ has rank d^*. Write $\varphi = (t_1, \ldots, t_d)$ and consider the function $f\colon \mathbb{Z}^\ell \to \mathbb{C}$ given by

$$f(s_1, \ldots, s_\ell) = \sum_{\substack{1 \le i \le d \\ 1 \le j \le \ell}} t_i s_j \lambda_{ij}.$$

By construction, it maps elements of $\mathcal{E}$ to elements of $2\pi\sqrt{-1}\mathbb{Z}$ of absolute value $\leq c_0 SF|\varphi|$. On the other hand, since $\ell \geq d$ and $\ell \geq 3$, we have $S^{\ell-1} \geq c_0^3 T^{d-1} F$, and so,

$$\mathrm{Card}(\mathcal{E}) \geq \frac{S^\ell \det(\Phi)}{d! c_0 T^{d-1}} > c_0 SF|\varphi|.$$

Thus, f is not injective on $\mathcal{E}$ and so, there exists a nonzero element $(s_1, \ldots, s_\ell)$ of $\mathbb{Z}^\ell$ with $|s_j| < 2S$, $(0 \leq j \leq \ell)$, such that $f(s_1, \ldots, s_\ell) = 0$. We deduce

$$\Big|\sum_{i=1}^{d} t_i \lambda_{i1} \sum_{j=1}^{\ell} s_j \lambda_{1j}\Big| = \Big|\sum_{i=1}^{d}\sum_{j=1}^{\ell} t_i s_j (\lambda_{i1}\lambda_{1j} - \lambda_{11}\lambda_{ij})\Big| \leq e^{-V}. \tag{7.1}$$

Since $\lambda_{11}, \ldots, \lambda_{d1}$ are linearly independent over $\mathbb{Q}$ and since $\lambda_{11}, \ldots, \lambda_{1\ell}$ are also linearly independent over $\mathbb{Q}$, none of the numbers $\sum_{i=1}^{d} t_i \lambda_{i1}$ and $\sum_{j=1}^{\ell} s_j \lambda_{1j}$ vanishes. Moreover, we have

$$|\varphi| = \max_{1 \leq i \leq d} |t_i| \leq T,$$

because G^* is defined by polynomials of partial degrees $\leq T$. Thus, Liouville's inequality yields lower bounds:

$$\Big|\sum_{i=1}^{d} t_i \lambda_{i1}\Big| \geq \frac{1}{2} \min\Big\{1, \Big|1 - \prod_{i=1}^{d} \gamma_{i1}^{t_i}\Big|\Big\} \geq \exp\{-c_0 TDh\}$$

and similarly

$$\Big|\sum_{j=1}^{\ell} s_j \lambda_{1j}\Big| \geq \exp\{-c_0 SDh\}.$$

Since $V > c_0 TSDh$, this is a contradiction.

Finally, assume $d^* = d$. In this case, the subgroup G^* is reduced to the neutral element of G, and we have $\Phi = \mathbb{Z}^d$. Since $S^\ell \geq c_0^2 T^d$, we get $\mathrm{Card}(\mathcal{E}) > 1$. Let $\mathbf{s} = (s_1, \ldots, s_\ell)$ be a nonzero element of $\mathcal{E}$. For each $(t_1, \ldots, t_d) \in \mathbb{Z}^d$ with $0 \leq t_i < T$, $(1 \leq i \leq d)$, the sum

$$\sum_{i=1}^{d}\sum_{j=1}^{\ell} t_i s_j \lambda_{ij} \tag{7.2}$$

is an element of $2\pi\sqrt{-1}\mathbb{Z}$ of absolute value $\leq c_0 TSDh/E$. Since $c_0 TSDh/E < T^d$, Dirichlet's box principle yields a point $\mathbf{t} = (t_1, \ldots, t_d) \in \mathbb{Z}^d$ with $|t_i| < T$, $(1 \leq i \leq d)$, for which the sum (7.2) vanishes. For these choices of $\mathbf{s}$ and $\mathbf{t}$, inequality (7.1) again holds, and we get a contradiction as above. ∎

A direct proof of Theorem 2.3 can be given along the same lines. It shows that the technical hypothesis can be replaced by the following weaker one: *the numbers $x_1, \ldots, x_d$ satisfy a measure of linear independence with exponent d, and the numbers $y_1, \ldots, y_\ell$ satisfy a measure of linear independence of exponent ℓ.*

Here, we prefer to derive Theorem 2.3 from Theorem 2.4, in order to show the link between the two results. To this end, we will need the following lemma:

Lemma 7.1. – *Let $z_1, \ldots, z_n$ be complex numbers satisfying a measure of linear independence with exponent $\nu > 0$, and let $\theta > 3n\nu$ be a real number. There exists a positive constant c satisfying the following property. Let $\lambda_1, \ldots, \lambda_n$ be logarithms of algebraic numbers, let D be a positive integer, and let $h \geq c$ be a real number. Define $\gamma_j = e^{\lambda_j}$, $(1 \leq j \leq n)$, and assume*

$$[\mathbb{Q}(\gamma_1, \ldots, \gamma_n) : \mathbb{Q}] \leq D, \qquad \max\{\mathrm{h}(\gamma_j), |\lambda_j|\} \leq h, \quad (1 \leq j \leq n),$$

and

$$\max_{1 \leq j \leq n} |z_j - \lambda_j| \leq \exp\{-(Dh)^\theta\}.$$

Then the numbers $\lambda_1, \ldots, \lambda_n$ are $\mathbb{Q}$-linearly independent.

Proof. By assumption there exists a real number T_0 such that, for $T \geq T_0$ and for $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ satisfying

$$0 < \max\{|t_1|, \ldots, |t_n|\} \leq T,$$

the inequality

$$|t_1 z_1 + \cdots + t_n z_n| \geq \exp\{-T^\nu\}$$

holds. Since $\nu < \theta/(3n)$, we may assume

$$T^\nu + \log(nT) < T^{\theta/(3n)}$$

for $T \geq T_0$. Suppose $h \geq c$ where

$$c_1(n) = (10^3 n)^{n-1} \quad \text{and} \quad c = \max\{c_1(n)^{1/(2n)}, T_0^{1/(3n)}\}.$$

If the numbers $\lambda_1, \ldots, \lambda_n$ were linearly dependent over $\mathbb{Q}$, we could use Lemma 7.2 of [32] and write

$$t_1\lambda_1 + \cdots + t_n\lambda_n = 0,$$

with a n-tuple $(t_1, \ldots, t_n) \in \mathbb{Z}^n$ such that

$$0 < \max\{|t_1|, \ldots, |t_n|\} \leq c_1(n)(D^3 h)^{n-1}.$$

Put $T = (Dh)^{3n}$. Then, we get $T \geq T_0$, $\max\{|t_1|, \ldots, |t_n|\} \leq T$, and

$$|t_1 z_1 + \cdots + t_n z_n| \leq nT \max_{1 \leq j \leq n} |x_j - \lambda_j| \leq nT \exp\left\{ - T^{\theta/(3n)}\right\} < \exp\left\{ - T^\nu\right\},$$

which contradicts the hypothesis on the measure of linear independence of $z_1, \ldots, z_n$. □

Proof of Theorem 2.3. Let D be a positive integer, let c_2 and h be real numbers with $h \geq c_2^2 \geq 3$, and let $\gamma_{11}, \dots, \gamma_{d\ell}$ be algebraic numbers which generate over $\mathbb{Q}$ a field K of degree $\leq D$, and satisfy $h(\gamma_{ij}) \leq h$ for $i = 1, \dots, d$ and $j = 1, \dots, \ell$. Suppose

$$\left|\gamma_{ij} - e^{x_i y_j}\right| \leq e^{-3V} \quad \text{where} \quad V = c_2^{\kappa+1}(Dh)^{\kappa}(\log D + \log h)^{1-\kappa}.$$

We will derive a contradiction, assuming that c_2 is sufficiently large as a function of $x_1, \dots, x_d$ and $y_1, \dots, y_\ell$.

For this purpose, we may assume, without loss of generality, that K has degree exactly D over $\mathbb{Q}$. For each $i = 1, \dots, d$ and $j = 1, \dots, \ell$, choose a determination λ_{ij} of the logarithm of γ_{ij} so that

$$|\lambda_{ij} - x_i y_j| \leq e^{-2V}.$$

We get

$$\max_{\substack{1 \leq i \leq d \\ 1 \leq j \leq \ell}} |\lambda_{ij}\lambda_{11} - \lambda_{i1}\lambda_{1j}| \leq e^{-V}.$$

Moreover, since $x_1 y_1, \dots, x_d y_1$ satisfy a measure of linear independence with exponent $< \kappa/(3d)$, Lemma 7.1 shows that $\lambda_{11}, \dots, \lambda_{d1}$ are linearly independent over $\mathbb{Q}$. Similarly, since $x_1 y_1, \dots, x_1 y_\ell$ satisfy a measure of linear independence with exponent $< \kappa/(3\ell)$, Lemma 7.1 shows that $\lambda_{11}, \dots, \lambda_{1\ell}$ are linearly independent over $\mathbb{Q}$. The contradiction follows by applying Theorem 2.4 with $E = Dh/c_2$. Note that $E \geq (Dh)^{1/2}$ since $h \geq c_2^2$. ∎

§8. Proof of Theorems 2.5 and 2.6

In this section we give a lower bound for $\sum |\beta_j - \log \alpha_j|$ and we deduce Theorems 2.5 and 2.6.

Theorem 8.1. – *Let n be a positive integer. There exist two positive constants c_1 and c_2 with the following property. Let $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$ be algebraic numbers, let D be the degree of the number field they generate, and let A, B, B', E be real numbers which are $\geq e$ and satisfy*

$$\max_{1 \leq j \leq n} \mathrm{h}(\alpha_j) \leq \log A \quad \textit{and} \quad \max_{1 \leq j \leq n} \mathrm{h}(\beta_j) \leq \log B.$$

For $1 \leq j \leq n$, assume that the number α_j does not vanish, and choose a determination λ_j of its logarithm. Assume

$$\max_{1 \leq j \leq n} |\lambda_j| \leq \frac{D}{E} \log A,$$

$$\log E \leq D \log A, \quad \log E \leq D \log B, \quad \log E \leq D \log B', \tag{8.1}$$

$$D(\log A)(\log B) \geq (\log B')(\log E), \tag{8.2}$$

$$B \geq D(\log B')(\log E)^{-1} \quad \textit{and} \quad B' \geq D(\log A)(\log B). \tag{8.3}$$

Furthermore, assume

$$s_1\beta_1 + \cdots + s_n\beta_n \neq 0$$

for any $(s_1, \ldots, s_n) \in \mathbb{Z}^n$ *with*

$$0 < \max_{1\leq j\leq n} |s_j| \leq c_1\Big(\frac{D\log B'}{\log E}\Big)^{1/n}.$$

Then, we have

$$\sum_{j=1}^{n} |\beta_j - \lambda_j| \geq \exp\big\{ - c_2 D^{2+1/n}(\log A)(\log B)(\log B')^{1/n}(\log E)^{-1-1/n}\big\}.$$

Proof. Let $c_0 \geq 1$ be a real number. Set

$$V = c_0^{5+4/n} D^{2+1/n}(\log A)(\log B)(\log B')^{1/n}(\log E)^{-1-1/n}.$$

Assume $c_1 \geq c_0^{5/n}$ and

$$\sum_{j=1}^{n} |\beta_j - \lambda_j| < e^{-2V}.$$

We will show that, if c_0 is sufficiently large as a function of n, then the last inequality leads to a contradiction. This will prove the theorem with $c_2 = 2c_0^{5+4/n}$.

To this end, we apply Theorem 5.1 with the group $G = \mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}$, so that $d_0 = d_1 = 1$ and $d = 2$. For the number field K, we take $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$. Its degree over $\mathbb{Q}$ is D. We choose the points

$$w_1' = w_1 = (1, 1), \quad \eta_j' = (\beta_j, \beta_j), \quad \eta_j = (\beta_j, \lambda_j), \qquad (1 \leq j \leq n),$$

so that $\ell_0 = 1$ and $\ell_1 = n$ and $r = 1$. Note that n has a different meaning here than in the statement of Theorem 5.1. Let Γ be the subgroup of $G(K) = K \times K^\times$ generated by

$$\gamma_j = \exp_G(\eta_j) = (\beta_j, \alpha_j), \qquad (1 \leq j \leq n).$$

We use the parameters

$$B_1 = B^{c_0}, \quad B_2 = (B')^{c_0}, \quad U = c_0^{-1}V, \quad T_0 = \Big[\frac{U}{D\log B_1}\Big], \quad S_0 = \Big[\frac{U}{D\log B_2}\Big],$$

$$T_1 = \left[c_0^2 \frac{D \log B_1}{\log E}\right], \quad S_1 = \ldots = S_n = S = \left[\left(c_0^3 \frac{D \log B_2}{\log E}\right)^{1/n}\right] \quad \text{and} \quad A_1 = A^{c_0 S}.$$

By (8.1), the integers T_0, T_1 and S are positive. The inequality (8.2) combined with (8.1) gives as well

$$S_0 \geq \left[c_0^{3+4/n}\left(\frac{D \log B'}{\log E}\right)^{1/n}\right] \geq 1.$$

Assuming c_0 sufficiently large, the left inequality in (8.3) gives $S \leq (c_0^4 B)^{1/n} \leq B_1^{1/2}$, thus

$$\log(nS) + \sum_{j=1}^{n} \mathrm{h}(\beta_j) \leq \frac{1}{2}\log B_1 + \log n + n \log B \leq \log B_1.$$

Using the right inequality in (8.3), we also find $U \leq B_2$. So, we get

$$2S_0 + T_0 + T_1 \leq U \leq B_2.$$

The remaining conditions of Theorem 5.1 are plainly satisfied.

Therefore, there is a connected algebraic subgroup G^* of G, distinct from G, such that

$$S_0 \operatorname{Card}\left(\frac{\Gamma(S) + G^*(K)}{G^*(K)}\right) \mathcal{H}(G^*\,; T_0, T_1) \leq 2T_0T_1.$$

Here, the exponent ℓ_0^* of S_0 is 1 because the only possibilities for G^* are $\{0\}\times\{1\}$, $\{0\}\times\mathbb{G}_{\mathrm{m}}$, or $\mathbb{G}_{\mathrm{a}} \times \{1\}$, and, in all cases, w_1 does not belong to the tangent space of G^* at the identity. Since

$$2T_0T_1 \leq 2c_0^2 \frac{U}{\log E} < S_0 S^n,$$

this inequality implies

$$\operatorname{Card}\left(\frac{\Gamma(S) + G^*(K)}{G^*(K)}\right) \mathcal{H}(G^*\,; T_0, T_1) < S^n. \tag{8.4}$$

Explicitly, we have

$$\Gamma(S) = \left\{(s_1\beta_1 + \cdots + s_n\beta_n, \alpha_1^{s_1}\cdots\alpha_n^{s_n})\,;\, 0 \leq s_j < S,\ (1 \leq j \leq n)\right\}.$$

Since $c_1 \geq c_0^{5/n}$, the hypothesis tells us that, for any nonzero element $\mathbf{s} = (s_1, \ldots, s_n)$ of $\mathbb{Z}^n$ with $|\mathbf{s}| < 2S$, we have

$$s_1\beta_1 + \cdots + s_n\beta_n \neq 0.$$

Thus, the set

$$\left\{s_1\beta_1 + \cdots + s_n\beta_n\,;\, 0 \leq s_j < S,\ 1 \leq j \leq n\right\}$$

has cardinality S^n. Since this set is the projection of $\Gamma(S)$ on the factor $\mathbb{G}_{\mathrm{a}}$ of G, the condition (8.4) is not satisfied if G^* is equal to $\{0\} \times \{1\}$ or $\{0\} \times \mathbb{G}_{\mathrm{m}}$. It remains the case where $G^* = \mathbb{G}_{\mathrm{a}} \times \{1\}$. In this case, the condition (8.4) becomes

$$\mathrm{Card}\bigl\{\alpha_1^{s_1} \cdots \alpha_n^{s_n}\,;\, 0 \le s_j < S,\; 1 \le j \le n\bigr\} < \frac{S^n}{T_0}.$$

Let $\mathcal{E}$ be the set of all points $(s_1, \ldots, s_n) \in \mathbb{Z}^n$ with supremum norm $< S$ such that $\alpha_1^{s_1} \cdots \alpha_n^{s_n} = 1$. Since

$$\mathrm{Card}\bigl\{\alpha_1^{s_1} \cdots \alpha_n^{s_n}\,;\, 0 \le s_j < S,\; 1 \le j \le n\bigr\} \ge \frac{S^n}{\mathrm{Card}(\mathcal{E})},$$

we get $\mathrm{Card}(\mathcal{E}) > T_0$. On the other hand, for each $(s_1, \ldots, s_n) \in \mathcal{E}$, we have

$$s_1\lambda_1 + \cdots + s_n\lambda_n = 2\pi\sqrt{-1}\, s_0,$$

for an integer s_0 with

$$|s_0| \le \frac{nS}{2\pi} \max_{1 \le j \le n} |\lambda_j| \le \frac{nSD\log A}{2\pi E} \le \frac{c_0 SD\log A}{\log E} \le c_0^{-1} T_0.$$

By Dirichlet box principle, this means that there are at least two different elements of $\mathcal{E}$ with the same value of s_0. Taking their difference, we get a nonzero element $\mathbf{s} = (s_1, \ldots, s_n)$ of $\mathbb{Z}^n$ with $|\mathbf{s}| < 2S$ such that

$$s_1\lambda_1 + \cdots + s_n\lambda_n = 0.$$

This implies

$$\bigl|s_1\beta_1 + \cdots + s_n\beta_n\bigr| \le 2nSe^{-2V} \le e^{-V}.$$

Since $s_1\beta_1 + \cdots + s_n\beta_n$ is a nonzero algebraic number with absolute logarithmic height $\le \log(2nS) + n\log B \le \log(2B_1)$, Liouville's inequality gives

$$\bigl|s_1\beta_1 + \cdots + s_n\beta_n\bigr| \ge (2B_1)^{-D}.$$

This is impossible since $V \ge c_0 D \log B_1$. This contradiction ends the proof. $\square$

Remark. Here, we applied Theorem 2.1 of [21] with the algebraic group $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}$, the direction $(1,1)$ and the n points $(\beta_1, \lambda_1), \ldots, (\beta_n, \lambda_n)$. A similar argument can be given with the algebraic group $\mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}^n$, the direction $(1, \beta_1, \ldots, \beta_n)$ and a single point $(1, \lambda_1, \ldots, \lambda_n)$. The choice of parameters is similar but the conditions which arise concerning B and B' are not exactly the same. The transition from one proof to the other is merely the transposition of the interpolation matrix. Compare with the remark a) in section 7 of [33].

Proof of Theorem 2.5
Let $D \geq 1$ be an integer, and let $h \geq e$ be a real number. Put

$$\varphi(D,h) = 16c_2 D^{2+1/n} h(h+\log D)(\log h + \log D)^{-1},$$

where c_2 is as in Theorem 8.1. Assume that $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$ are algebraic numbers in a number field of degree $\leq D$, which satisfy

$$\max_{1\leq j\leq n} \mathrm{h}(\alpha_j) \leq h \quad \text{and} \quad \max_{1\leq j\leq n} \mathrm{h}(\beta_j) \leq h.$$

We will show that, if h is sufficiently large, with a lower bound depending only on $x_1, \ldots, x_n$, then we have

$$\max_{1\leq j\leq n} \max\{|x_j - \beta_j|, |e^{x_j} - \alpha_j|\} \geq \exp\{-\varphi(D,h)\}. \tag{8.5}$$

We argue by contradiction, assuming that (8.5) does not hold. Since $\varphi(D,h)$ is an increasing function of D, we may assume, that D is the degree of the extension of $\mathbb{Q}$ generated by $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$. For $j = 1, \ldots, n$, denote by λ_j the determination of the logarithm of α_j which is closest to x_j. If h is sufficiently large, we obtain

$$\sum_{j=1}^n |\beta_j - \lambda_j| < \exp\{-(1/2)\varphi(D,h)\}.$$

Define

$$A = e^h, \quad B = De^h, \quad B' = (Dh)^2 \quad \text{and} \quad E = (Dh)^{1/2}.$$

Then, if h is sufficiently large, all the hypotheses of Theorem 8.1 are satisfied, except maybe the condition about linear combinations of $\beta_1, \ldots, \beta_n$. Moreover, the conclusion of the theorem fails. Therefore, there are integers $s_1, \ldots, s_n$ with

$$\sum_{j=1}^n s_j \beta_j = 0 \quad \text{and} \quad 0 < \max_{1\leq j\leq n} |s_j| \leq c_1 (4D)^{1/n}.$$

This implies

$$\Bigl|\sum_{j=1}^n s_j x_j\Bigr| \leq 4nc_1 D^{1/n} \exp\{-\varphi(D,h)\} \tag{8.6}$$

which contradicts the hypothesis that $x_1, \ldots, x_n$ satisfy a measure of linear independence with exponent $2n+1$. $\square$

Remark. Note that, for fixed D, we get only finitely many possibilities for $(s_1, \ldots, s_n)$. For each of them, (8.6) cannot hold if h is sufficiently large. This does not require that $x_1, \ldots, x_n$ satisfy a measure of linear independence but simply that they be linearly independent over $\mathbb{Q}$. Thus, (8.5) holds with this weaker condition for $h \geq h_0(D, x_1, \ldots, x_n)$.

Proof of Theorem 2.6

Let $D \in \mathbb{N}$ and $h \in \mathbb{R}$ satisfy $D \geq 1$ and $h \geq e$. Assume that there exist algebraic numbers $\alpha_1, \ldots, \alpha_n$ such that

$$[\mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) : \mathbb{Q}] \leq D, \qquad \max_{1 \leq j \leq n} \mathrm{h}(\alpha_j) \leq h$$

and

$$\max_{1 \leq j \leq n} |e^{\beta_j} - \alpha_j| < \exp\bigl\{-8c_2 D^{1+(1/n)} h(\log h + D \log D)(\log h + \log D)^{-1}\bigr\}$$

with c_2 as in Theorem 8.1. It remains to show that this is impossible if h is larger than some constant h_0 depending only on $\beta_1, \ldots, \beta_n$. The argument is similar to the proof of Theorem 2.5. We may again assume that D is the degree of the number field generated by $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$. Set

$$A = e^h, \qquad B = Dh^{1/D}, \qquad B' = (Dh)^2, \qquad E = (Dh)^{1/2}.$$

Since $\beta_1, \ldots, \beta_n$ are linearly independent over $\mathbb{Q}$, Theorem 8.1 yields the desired contradiction. $\square$

Remark. It is possible to refine Theorem 8.1 in such a way as to include Fel'dman's simultaneous approximation measure for logarithms of algebraic numbers. A slight modification of the proof in [33] is needed (cf. [33], § 7, subsection e), where the basis $1, z, \ldots, z^n$ of the space of polynomials of degree $\leq n$ is replaced by $z(z-1)\cdots(z-j+1)/j!$, $(0 \leq j \leq n)$. See [9], Lemma 19.7, p. 127.

§9. Proof of Theorem 2.7

Let c_0 be a real number ≥ 1, and let γ_1 and γ_2 be algebraic numbers. Put $\alpha = e^\lambda$, and define

$$K = \mathbb{Q}(\alpha, \beta, \gamma_1, \gamma_2), \quad D = [K : \mathbb{Q}] \quad \text{and} \quad h = \max\{3, \mathrm{h}(\gamma_1), \mathrm{h}(\gamma_2)\}.$$

Suppose

$$|\lambda - \gamma_1| + |e^{\beta\lambda} - \gamma_2| \leq e^{-3V}$$

where

$$V = c_0^6 D^2 h (h + \log D)^{1/2} (\log h + \log D)^{-1/2}.$$

We will derive a contradiction assuming, at each step, that c_0 is sufficiently large as a function of β and λ alone.

Let $mX^2 - bX - a$ be the irreducible polynomial of β over $\mathbb{Z}$, and denote by $\log \gamma_2$ the determination of the logarithm of γ_2 which satisfies

$$|\beta\lambda - \log \gamma_2| \le c_0 e^{-3V}.$$

We apply Theorem 5.1 to the group $G = \mathbb{G}_{\mathrm{a}} \times \mathbb{G}_{\mathrm{m}}^2$ with the points

$$\begin{aligned} w_1' &= (1, 1, \beta), & w_1 &= (1, 1, \beta), \\ \eta_1' &= \big(\lambda,\, \lambda,\, \beta\lambda\big), & \eta_1 &= \big(\gamma_1,\, \lambda,\, \log \gamma_2\big), \\ \eta_2' &= \big(m\beta\lambda,\, m\beta\lambda,\, m\beta^2\lambda\big), & \eta_2 &= \big(m\beta\gamma_1,\, m \log \gamma_2,\, a\lambda + b \log \gamma_2\big). \end{aligned}$$

So, we have $d_0 = \ell_0 = 1$, $d_1 = \ell_1 = 2$, $d = 3$ and $r = 1$. The group $G(K)$ is $K \times (K^\times)^2$, and its subgroup Γ is generated by

$$\exp_G(\eta_1) = \big(\gamma_1,\, \alpha,\, \gamma_2\big) \quad \text{and} \quad \exp_G(\eta_2) = \big(m\beta\gamma_1,\, \gamma_2^m,\, \alpha^a \gamma_2^b\big).$$

Put

$$S = \left[c_0^2 \sqrt{D} \right], \qquad U = c_0^{-1} V,$$

and define the remaining parameters by

$$A_1 = A_2 = e^{c_0 S h}, \quad B_1 = (De^h)^{c_0}, \quad B_2 = (Dh)^{c_0}, \quad E = Dh,$$

$$T_0 = \left[\frac{U}{c_0 D (h + \log D)} \right], \quad T_1 = T_2 = T = \left[\frac{U}{c_0^{7/2} D^{3/2} h} \right],$$

$$S_0 = \left[\frac{U}{c_0 D (\log h + \log D)} \right] \quad \text{and} \quad S_1 = S_2 = S.$$

Then, all conditions of Theorem 5.1 are satisfied. In particular, the main condition (5.4) holds and we have

$$S_0 S^2 > 6 T_0 T^2 \quad \text{and} \quad S_0 S > 6T^2.$$

Moreover, $\Gamma(S)$ is the set of points

$$\big((s_1 + m s_2 \beta)\gamma_1,\, \alpha^{s_1} \gamma_2^{m s_2},\, \alpha^{a s_2} \gamma_2^{s_1 + b s_2}\big), \qquad (0 \le s_1, s_2 < S).$$

By Theorem 5.1, there is a connected algebraic subgroup G^* of G, of dimension ≤ 2, such that
$$S_0 \,\mathrm{Card}\left(\frac{\Gamma(S)+G^*(K)}{G^*(K)}\right)\mathcal{H}(G^*;T_0,T_1,T_2)\leq 6T_0T^2.$$

The exponent of S_0 in the left hand side is 1 because, since β is irrational, there is no algebraic subgroup of G, apart from G itself, whose tangent space at the origin contains $w_1=(1,1,\beta)$. Write $G^*=G_0^*\times G_1^*$ where G_0^* is an algebraic subgroup of $\mathbb{G}_{\mathrm{a}}$ and G_1^* is an algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^2$. The factor G_0^* is either $\{0\}$ or $\mathbb{G}_{\mathrm{a}}$. If we had $G_0^*=\{0\}$, then, since $\beta\notin\mathbb{Q}$ and $\gamma_1\neq 0$, we would get

$$\mathrm{Card}\left(\frac{\Gamma(S)+G^*(K)}{G^*(K)}\right)\geq S^2>6T_0T^2/S_0,$$

which is not possible. Hence, we have $G^*=\mathbb{G}_{\mathrm{a}}\times G_1^*$ and G_1^* is an algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^2$ of dimension ≤ 1. Denote by $\Gamma_1(S)$ the projection of $\Gamma(S)$ on the factor $\mathbb{G}_{\mathrm{m}}^2$ of G. This set consists of the points

$$\bigl(\alpha^{s_1}\gamma_2^{ms_2},\,\gamma_2^{s_1}(\alpha^a\gamma_2^b)^{s_2}\bigr),\qquad (0\leq s_1,s_2<S).$$

Then, we find
$$\mathrm{Card}\left(\frac{\Gamma_1(S)+G_1^*(K)}{G_1^*(K)}\right)\leq 6T^2/S_0<S.$$

This last inequality shows that the images of (α,γ_2) and $(\gamma_2^m,\alpha^a\gamma_2^b)$ in the quotient $(K^\times)^2/G_1^*(K)$ are torsion points (of order $<S$). Thus, there exist integers k_1, k_2, not both zero, such that
$$\alpha^{k_1}\gamma_2^{k_2}=1\quad\text{ and }\quad\gamma_2^{mk_1}(\alpha^a\gamma_2^b)^{k_2}=1.$$

We deduce
$$(\gamma_2)^{mk_1^2+bk_1k_2-ak_2^2}=1.$$

The polynomial $mX^2-bXY-aY^2$ being irreducible over $\mathbb{Q}$, this exponent is nonzero, and so, γ_2 is a root of unity. It follows that α is also a root of unity. Since γ_2 belongs to K and since K has degree D over $\mathbb{Q}$, the order of γ_2 must be $\leq 2D^2$. Write $(\log\gamma_2)/\lambda=p/q$ with relatively prime integers p and q with $q>0$. Since λ is fixed, we get $q<c_0D^2$, and, because β is quadratic irrational, Liouville's inequality yields

$$|\beta\lambda-\log\gamma_2|\geq\frac{1}{c_0q^2}\geq\frac{1}{c_0^3D^4},$$

in contradiction with the choice of $\log\gamma_2$. $\square$

§10. Proof of Theorem 2.8

Denote by $\mathcal{L}$ the $\mathbb{Q}$-vector space of logarithms of algebraic numbers:

$$\mathcal{L} = \exp^{-1}(\overline{\mathbb{Q}}^{\times}).$$

The main result of this section is the following:

Theorem 10.1. – *Let d_1 and ℓ_1 be positive integers and let $M = (\lambda_{ij})$ be a $d_1 \times \ell_1$ matrix with coefficients in $\mathcal{L}$. Set $\kappa = (1/d_1) + (1/\ell_1)$. Denote by X the $\mathbb{Q}$-vector subspace of $\mathbb{C}^{d_1}$ which is spanned by the columns of M. Let r be the rank of M. Assume that, for any surjective linear map $g : \mathbb{C}^{d_1} \to \mathbb{C}^{d_1^*}$ which is defined over $\mathbb{Q}$, the dimension ℓ_1^* of the $\mathbb{Q}$-vector space $g(X)$ satisfies*

$$\ell_1^*/\ell_1 \geq d_1^*/d_1.$$

Then, there exists a positive constant C such that the function

$$CD^{r\kappa+1}(h + \log D)^{r\kappa+1}(\log D)^{-r\kappa-1}$$

is a measure of simultaneous approximation for the $d_1\ell_1$ numbers λ_{ij}, $(1 \leq i \leq d_1,\ 1 \leq j \leq \ell_1)$.

Note that under the hypotheses of this theorem, we have $r\kappa \geq 1$ by virtue of Corollary 7.2 of [30].

Proof. Let D be a positive integer, let c_0 and h be positive real numbers with $h \geq c_0 \geq 3$, and let γ_{ij}, $(1 \leq i \leq d_1,\ 1 \leq j \leq \ell_1)$, be algebraic numbers. Assume that the number field K generated over $\mathbb{Q}$ by the $2d_1\ell_1$ numbers

$$\alpha_{ij} := e^{\lambda_{ij}}, \quad \gamma_{ij}, \qquad (1 \leq i \leq d_1, \quad 1 \leq j \leq \ell_1)$$

has degree $\leq D$. Suppose also

$$\max_{\substack{1\leq i\leq d_1\\1\leq j\leq \ell_1}} \mathrm{h}(\gamma_{ij}) \leq h \quad \text{and} \quad \max_{\substack{1\leq i\leq d_1\\1\leq j\leq \ell_1}} |\lambda_{ij} - \gamma_{ij}| \leq \exp(-2V)$$

where

$$V = c_0^{3+4r\kappa}\left(\frac{D(h+\log D)}{\log(eD)}\right)^{r\kappa+1}.$$

Note that, since $r\kappa \geq 1$, we have $V \geq c_0^{3+4r\kappa}D(h + \log D)$. We will derive a contradiction assuming, at each step, that c_0 is a sufficiently large constant, independent of h, D and the algebraic numbers γ_{ij}. This will prove the theorem.

Without loss of generality, we may assume $D = [K : \mathbb{Q}]$. By permuting the rows and columns of M, we may also assume that the principal minor of order r of M is nonzero:

$$\det(\lambda_{ij})_{1 \le i,j \le r} \neq 0.$$

We claim that the matrix $M' = (\gamma_{ij})$ also has rank r, and that its principal minor of order r is nonzero. To justify this, let I be a subset of $\{1, \dots, d_1\}$ and let J be a subset of $\{1, \dots, \ell_1\}$, both with the same cardinality. We find

$$\left| \det(\lambda_{ij})_{i \in I, j \in J} - \det(\gamma_{ij})_{i \in I, j \in J} \right| \le c_0 \exp(-2V) < \exp(-V).$$

Since there are only finitely many possibilities for I and J, we deduce $\det(\gamma_{ij})_{i \in I, j \in J} \neq 0$ if $\det(\lambda_{ij})_{i \in I, j \in J} \neq 0$. Conversely, if $\det(\gamma_{ij})_{i \in I, j \in J} \neq 0$, then Liouville's inequality gives

$$\left| \det(\gamma_{ij})_{i \in I, j \in J} \right| \ge \exp(-c_0 D h).$$

Since $V > c_0 D h$, this implies $\det(\lambda_{ij})_{i \in I, j \in J} \neq 0$. So, a minor of M vanishes if and only if the corresponding minor of M' vanishes.

We apply Theorem 5.1 to the group $G = \mathbb{G}_{\mathrm{a}}^r \times \mathbb{G}_{\mathrm{m}}^{d_1}$. So, we have $d_0 = r$ and $d = r + d_1$. We also choose $\ell_0 = \ell_1$ and define four families of ℓ_1 points by

$$\begin{aligned} w'_j = \eta'_j &= (\lambda_{1j}, \dots, \lambda_{rj} \,;\, \lambda_{1j}, \dots, \lambda_{d_1 j}) \in T_G(\mathbb{C}) = \mathbb{C}^d, \\ w_j &= (\gamma_{1j}, \dots, \gamma_{rj} \,;\, \gamma_{1j}, \dots, \gamma_{d_1 j}) \in T_G(K) = K^d, \qquad (1 \le j \le \ell_1). \\ \eta_j &= (\gamma_{1j}, \dots, \gamma_{rj} \,;\, \lambda_{1j}, \dots, \lambda_{d_1 j}) \in T_G(\mathbb{C}) = \mathbb{C}^d, \end{aligned}$$

By construction, the subspace of $\mathbb{C}^d$ generated by $w'_1, \dots, w'_{\ell_1}$ and $\eta'_1, \dots, \eta'_{\ell_1}$ has dimension r. So, there is no conflict of notations concerning this parameter r. Consider the matrices

$$\mathbb{L}' = \begin{pmatrix} M & M \\ M & M \end{pmatrix} \quad \text{and} \quad \mathbb{L} = \begin{pmatrix} M' & M' \\ M' & M \end{pmatrix}.$$

The reader may also think of $w'_1, \dots, w'_{\ell_1}$ (resp. $w_1, \dots, w_{\ell_1}$) as the first ℓ_1 column vectors of $\mathbb{L}'$ (resp. $\mathbb{L}$), and of $\eta'_1, \dots, \eta'_{\ell_1}$ (resp. $\eta_1, \dots, \eta_{\ell_1}$) as their last ℓ_1 column vectors. We have $G(K) = K^r \times (K^\times)^{d_1}$, and the subgroup Γ of $G(K)$ is generated by the ℓ_1 points

$$\gamma_j = \exp_G(\eta_j) = (\gamma_{1j}, \dots, \gamma_{rj} \,;\, \alpha_{1j}, \dots, \alpha_{d_1 j}), \qquad (1 \le j \le \ell_1).$$

Finally, W is the subspace of $\mathbb{C}^d$ spanned by $w_1, \dots, w_{\ell_1}$. Define

$$B_1 = B_2 = B = (De^h)^{c_0}, \quad E = eD, \quad U = c_0^{-1} V, \quad T_0 = S_0 = \left[\frac{U}{D \log B} \right].$$

The last two parameters satisfy $T_0 = S_0 \geq c_0^{4r\kappa}$. Let T and S be the integers given by

$$T = \left[\left(c_0^2 \frac{D \log B_1}{\log E} \right)^{r/d_1} \right], \qquad S = \left[\left(c_0^3 \frac{D \log B_2}{\log E} \right)^{r/\ell_1} \right].$$

Since $\log E \leq D$, these integers as well are positive. For the remaining parameters, we choose

$$\log A_1 = \cdots = \log A_{d_1} = c_0 S, \quad T_1 = \cdots = T_{d_1} = T, \quad S_1 = \cdots = S_{\ell_1} = S.$$

Then, all the hypotheses of Theorem 5.1 are satisfied. Therefore, there exists a connected algebraic subgroup G^* of G, defined over K, incompletely defined in G by polynomials of degree $\leq T$ in each of the last ℓ_1 variables, and distinct from G, such that

$$S_0^{\ell_0^*} \operatorname{Card} \Big(\frac{\Gamma(S) + G^*(K)}{G^*(K)} \Big) \mathcal{H}(G^* \,; T_0, T, \ldots, T) \leq \frac{d!}{r!} T_0^r T^{d_1}, \tag{10.1}$$

where

$$\ell_0^* = \dim_K \big((W + T_{G^*}(K)) / T_{G^*}(K) \big).$$

Write $G^* = G_0^* \times G_1^*$ where G_0^* and G_1^* are algebraic subgroups of $\mathbb{G}_{\mathrm{a}}^r$ and $\mathbb{G}_{\mathrm{m}}^{d_1}$ respectively. Put

$$d_0^* = r - \dim G_0^* \quad \text{and} \quad d_1^* = d_1 - \dim G_1^*,$$

and denote by λ^* the largest integer for which there exist λ^* elements $\gamma_1^*, \ldots, \gamma_{\lambda^*}^*$ among $\gamma_1, \ldots, \gamma_{\ell_1}$ such that

$$\sum_{j=1}^{\lambda^*} s_j \gamma_j^* \notin G^*(K)$$

for any $(s_1, \ldots, s_{\lambda^*}) \in \mathbb{Z}^{\lambda^*}$ with $0 < \max_{1 \leq j \leq \lambda^*} |s_j| < S$. Then, $(\Gamma(S) + G^*(K))/G^*(K)$ has cardinality $\geq S^{\lambda^*}$, and (10.1) implies

$$S_0^{\ell_0^*} S^{\lambda^*} \leq d!\, T_0^{d_0^*} T^{d_1^*}.$$

Since $S_0 = T_0 \geq S$, this gives

$$S^{\ell_0^* + \lambda^* - d_0^*} \leq d!\, T^{d_1^*}.$$

Finally, since $S^{\ell_1} \geq (1/2) c_0^r T^{d_1}$, we deduce that either we have

$$\frac{\ell_0^* + \lambda^* - d_0^*}{\ell_1} < \frac{d_1^*}{d_1}, \tag{10.2}$$

or $\ell_0^* + \lambda^* - d_0^* = d_1^* = 0$.

Let Φ be the set of points $\varphi = (t_1, \ldots, t_{d_1}) \in \mathbb{Z}^{d_1}$ such that the monomial $Y_1^{t_1} \cdots Y_{d_1}^{t_{d_1}}$ induces the trivial character on G_1^*. Since G_1^* is incompletely defined in $\mathbb{G}_{\mathrm{m}}^{d_1}$ be polynomials of degree $\leq T$ in each variable, Lemma 4.8 of [21] shows that Φ admits a basis $\varphi_1, \ldots, \varphi_{d_1^*}$ with $|\varphi_k| \leq c_0 T$ for $k = 1, \ldots, d_1^*$. Write $\varphi_k = (t_{k1}, \ldots, t_{kd_1})$ for $k = 1, \ldots, d_1^*$, and denote by $g_1 \colon \mathbb{C}^{d_1} \to \mathbb{C}^{d_1^*}$ the linear map given by

$$g_1(u_1, \ldots, u_{d_1}) = \Big(\sum_{i=1}^{d_1} t_{1i} u_i, \ldots, \sum_{i=1}^{d_1} t_{d_1^* i} u_i \Big)$$

for any point $(u_1, \ldots, u_{d_1}) \in \mathbb{C}^{d_1}$. By construction, this map is surjective, defined over $\mathbb{Q}$, and its kernel is $T_{G_1^*}(\mathbb{C})$. Moreover, a point $\xi = (u_1, \ldots, u_{d_1}) \in \mathbb{C}^{d_1}$ satisfies

$$\exp_{\mathbb{G}_{\mathrm{m}}^{d_1}}(\xi) = \big(e^{u_1}, \ldots, e^{u_{d_1}} \big) \in G_1^*(K)$$

if and only if $g_1(\xi) \in \big(2\pi\sqrt{-1}\,\mathbb{Z} \big)^{d_1^*}$.

Denote by $\xi_1, \ldots, \xi_{\ell_1}$ the columns of the matrix M, and let X be the $\mathbb{Q}$-vector subspace of $\mathbb{C}^{d_1}$ that they generate. Denote by ℓ_1^* the dimension of $g_1(X)$ over $\mathbb{Q}$. Then, if (10.2) holds, the hypothesis of the theorem gives

$$\ell_1^* > \ell_0^* - d_0^* + \lambda^*. \tag{10.3}$$

We will show that, nor can this inequality hold, nor can we have $\ell_0^* + \lambda^* - d_0^* = d_1^* = 0$. The proof will then be complete.

To show this, choose a linear map $g_0 \colon \mathbb{C}^r \to \mathbb{C}^{d_0^*}$ defined over K whose kernel is $T_{G_0^*}(\mathbb{C})$, and define $g \colon \mathbb{C}^r \times \mathbb{C}^{d_1} \to \mathbb{C}^{d_0^*} \times \mathbb{C}^{d_1^*}$ to be the product map $g = (g_0, g_1)$. Since $T_{G^*}(\mathbb{C})$ is the kernel of g, we have

$$\ell_0^* = \dim g(W).$$

Define $\Omega^* = \{0\}^{d_0^*} \times \big(2\pi\sqrt{-1}\,\mathbb{Z} \big)^{d_1^*} \subset \mathbb{C}^{d_0^*} \times \mathbb{C}^{d_1^*}$. By construction, we also have, for any $(s_1, \ldots, s_{\ell_1}) \in \mathbb{Z}^{\ell_1}$,

$$\sum_{j=1}^{\ell_1} s_j \gamma_j \in G^*(K) \iff \sum_{j=1}^{\ell_1} s_j g(\eta_j) \in \Omega^*.$$

Thus, λ^* is also the largest integer for which there exist λ^* elements $\eta_1^*, \ldots, \eta_\lambda^*$ among $\eta_1, \ldots, \eta_{\ell_1}$ such that

$$\sum_{j=1}^{\lambda^*} s_j g(\eta_j^*) \notin \Omega^*$$

for any $(s_1, \ldots, s_{\lambda^*}) \in \mathbb{Z}^{\lambda^*}$ with $0 < \max_{1 \leq j \leq \lambda^*} |s_j| < S$.

Denote by

$$\pi_0 \colon \mathbb{C}^d \longrightarrow \mathbb{C}^r \qquad (\text{resp. } \pi_1 \colon \mathbb{C}^d \longrightarrow \mathbb{C}^{d_1})$$

the projection on the first r coordinates, (resp. on the last d_1 coordinates). Similarly, denote by

$$\pi_0^*\colon \mathbb{C}^{d_0^*} \times \mathbb{C}^{d_1^*} \longrightarrow \mathbb{C}^{d_0^*} \qquad (\text{resp. } \pi_1^*\colon \mathbb{C}^{d_0^*} \times \mathbb{C}^{d_1^*} \longrightarrow \mathbb{C}^{d_0^*})$$

the projection on the first d_0^* coordinates, (resp. on the last d_1^* coordinates). By construction, we have $\pi_0(W) = \mathbb{C}^r$. Since $g_0 \circ \pi_0 = \pi_0^* \circ g$, this implies $\pi_0^*(g(W)) = \mathbb{C}^{d_0^*}$, and thus

$$\ell_0^* = d_0^* + \dim\big(g(W) \cap \ker(\pi_0^*)\big). \tag{10.4}$$

If we had $\ell_0^* + \lambda^* - d_0^* = d_1^* = 0$, this would imply $\lambda^* = 0$ and $\Omega^* = \{0\}$, and so, the kernel $T_{G^*}(\mathbb{C})$ of g would contain $\eta_1, \ldots, \eta_{\ell_1}$. Since $d_1^* = 0$, this kernel would also contain $\{0\} \times \mathbb{C}^{d_1}$. So, it would be all of $\mathbb{C}^d$, in contradiction with the hypothesis $G^* \neq G$. It remains to show that (10.3) cannot hold.

For simplicity, assume that $g_1(\xi_1), \ldots, g_1(\xi_{\ell_1^*})$ are linearly independent over $\mathbb{Q}$. Since $\xi_j = \pi_1(\eta_j)$ for $j = 1, \ldots, \ell_1$, this implies that $g(\eta_1), \ldots, g(\eta_{\ell_1^*})$ also are linearly independent over $\mathbb{Q}$. By virtue of (10.4), we have $\ell_0^* - d_0^* + \lambda^* \geq \lambda^*$. So, (10.3) does not hold if $\lambda^* \geq \ell_1^*$. Assume $\lambda^* < \ell_1^*$, and define $m = \ell_1^* - \lambda^*$. Then, there exist m linearly independent elements $(s_{11}, \ldots, s_{1\ell_1^*})$,..., $(s_{m1}, \ldots, s_{m\ell_1^*})$ of $\mathbb{Z}^{\ell_1^*}$ with supremum norm $< S$ such that

$$\sum_{j=1}^{\ell_1^*} s_{kj} g(\eta_j) \in \Omega^*, \qquad (1 \leq k \leq m). \tag{10.5}$$

Let A be the $(d_0^* + d_1^*) \times m$ matrix whose column vectors are given by (10.5). Since these vectors are linearly independent over $\mathbb{Q}$ and belong to Ω^*, the first r rows of A are zero, and the rank of A is equal to m. Moreover, let A' be a non-singular square matrix consisting of rows of A of indices, say, $j_1, \ldots, j_m$. Then, since the coefficients of A' belong to $2\pi\sqrt{-1}\,\mathbb{Z}$, its determinant is an integral multiple of $(2\pi\sqrt{-1})^m$. Now, consider the matrix B of the same size as A, whose column vectors are

$$\sum_{j=1}^{\ell_1^*} s_{kj} g(w_j), \qquad (1 \leq k \leq m). \tag{10.6}$$

Then, B also has rank m. To prove this, denote by B' the square matrix formed by the rows of B of indices $j_1, \ldots, j_m$. The coefficients of A' being bounded above, in absolute value, by $c_0^2 TS$, and the distance between A and B being $\leq c_0^2 TS \exp(-2V)$, we get

$$|\det A' - \det B'| \leq c_0^{2m+1} (TS)^m \exp(-2V) < 1.$$

Since $|\det A'| \geq (2\pi)^m$, this implies $\det B' \neq 0$. Thus, B has rank m. Moreover, since η_j and w_j have the same first r coordinates for any j, the first d_0^* rows of A and B are the same, that is, equal to zero. Therefore, the vectors in (10.6) are m elements of W which are linearly independent over $\mathbb{C}$ and belong to $\ker \pi_0^*$. By virtue of (10.4), this gives $\ell_0^* \geq d_0^* + m$ and thus $\ell_0^* - d_0^* + \lambda^* \geq \lambda^* + m = \ell_1^*$. This shows that (10.3) does not hold. ∎

Remark. The proof simplifies notably when all the logarithms λ_{ij} are real. In this case, the condition $\exp_G(\eta) \in G^*$ is equivalent to $g(\eta) = 0$, and thus, we have $\lambda^* \geq \ell_1^*$. This inequality combined with $\ell_0^* \geq d_0^*$ show that (10.3) is impossible. Moreover, this does not require $S_0 \geq S$. This allows one to use a smaller value for V. The reader may check that, in this case, one can use

$$V = c_0^{3+4r\kappa} D \left(\frac{D(h + \log D)}{\log(eD)} \right)^{r\kappa}.$$

Thus, there exists a constant $C > 0$ such that

$$CD^{r\kappa+1}(h + \log D)^{r\kappa}(\log D)^{-r\kappa}$$

is a measure of approximation of the $d_1\ell_1$ numbers λ_{ij}.

Corollary 10.2. – *Let $W \subset \mathbb{C}^{2n}$ be the set of zeroes of the polynomial $X_1Y_1 + \cdots + X_nY_n$. Let $w = (x_1, \ldots, x_n, y_1, \ldots, y_n)$ be a point in $\mathcal{L}^{2n} \cap W$ which does not belong to any vector subspace of $\mathbb{C}^{2n}$, defined over $\mathbb{Q}$ and contained in W. Then there exists a positive constant C such that*

$$CD^2(h + \log D)^2(\log D)^{-2}$$

is a measure of simultaneous approximation for the $2n$ numbers $x_1, \ldots, x_n, y_1, \ldots, y_n$.

Put $N = 2^n$. The proof of Corollary 10.2 rests on the next lemma which involves the map

$$\theta_n : \mathbb{C}^{2n} \to \mathrm{Mat}_{N\times N}(\mathbb{C})$$

defined in [21] (see the remark at the end of § 7). This map has the form

$$\theta_n(v) = \begin{pmatrix} 0 & \psi_n(v) \\ \varphi_n(v) & 0 \end{pmatrix},$$

where φ_n and ψ_n are $\mathbb{C}$-linear maps from $\mathbb{C}^{2n}$ to $\mathrm{Mat}_{2^{n-1}\times 2^{n-1}}(\mathbb{C})$. The latter maps are defined by induction on n. For $n = 1$, they are given by

$$\varphi_1(x_1, y_1) = (x_1), \qquad \psi_1(x_1, y_1) = (y_1).$$

For $n \geq 1$ and $v' = (x_1, \ldots, x_{n+1}, y_1, \ldots, y_{n+1}) \in \mathbb{C}^{2n+2}$, we put

$$\varphi_{n+1}(v') = \begin{pmatrix} x_{n+1} I_{2^{n-1}} & \psi_n(v) \\ -\varphi_n(v) & y_{n+1} I_{2^{n-1}} \end{pmatrix},$$

$$\psi_{n+1}(v') = \begin{pmatrix} y_{n+1} I_{2^{n-1}} & -\psi_n(v) \\ \varphi_n(v) & x_{n+1} I_{2^{n-1}} \end{pmatrix},$$

where $v = (x_1, \ldots, x_n, y_1, \ldots, y_n)$, and where, for a positive integer m, I_m denotes the $m \times m$ identity matrix. The main properties of the map θ_n are that, for any $v \in \mathbb{C}^{2n}$ written as above, we have

$$\theta_n(v)^2 = (x_1 y_1 + \cdots + x_n y_n)^2 I_{2^n}$$

and that the matrix $\theta_n(v)$ has rank $\leq N/2$ when $v \in W$.

We will need the following lemma:

Lemma 10.3. – *Let W be as in Corollary 10.2, and let $w = (x_1, \ldots, x_n, y_1, \ldots, y_n)$ be a point of this hypersurface. Set $N = 2^n$ and denote by X the $\mathbb{Q}$-vector subspace of $\mathbb{C}^N$ which is spanned over $\mathbb{Q}$ by the column vectors of the matrix $\theta_n(w)$. Assume that there exists a vector subspace U of $\mathbb{C}^N$, defined over $\mathbb{Q}$, such that*

$$\dim_{\mathbb{Q}}(X/(X \cap U)) < \dim_{\mathbb{C}}(\mathbb{C}^N/U).$$

Then w belongs to a vector subspace of $\mathbb{C}^{2n}$, defined over $\mathbb{Q}$ and contained in W.

Proof. Define

$$\lambda = \dim_{\mathbb{Q}}(X/(X \cap U)) \quad \text{and} \quad \delta = \dim_{\mathbb{C}}(\mathbb{C}^N/U).$$

There exist two matrices P and Q in $\mathrm{GL}_N(\mathbb{Q})$ such that $P\theta_n(w)Q$ can be written in block form

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix},$$

where the matrix A has size $\delta \times \lambda$. Let E be the vector subspace of $\mathbb{C}^{2n}$ over $\mathbb{C}$ which consists of the points $v \in \mathbb{C}^{2n}$ such that $P\theta_n(v)Q$ can be written in block form

$$\begin{pmatrix} A(v) & 0 \\ B(v) & C(v) \end{pmatrix},$$

where the matrix $A(v)$ has size $\delta \times \lambda$. Then, E is defined over $\mathbb{Q}$ and contains w. Since $A(v)$ has rank $\leq \lambda$, the matrix $\theta_n(v)$, for $v \in E$, has rank $\leq \lambda + d - \delta < d$. Hence, we get $\det \theta_n(v) = 0$, so $v \in W$. This shows that E is contained in W. $\square$

Proof of Corollary 10.2.

We apply Theorem 10.1 with $d_1 = \ell_1 = N = 2^n$ and $M = \theta_n(w)$. Since the coefficients of $\theta_n(w)$ are

$$0, \pm x_1, \ldots, \pm x_{n-1}, x_n, \pm y_1, \ldots, \pm y_{n-1}, y_n, \tag{10.7}$$

they all belong to $\mathcal{L}$. As in Lemma 10.3, define X to be the $\mathbb{Q}$-vector space generated by the columns of $\theta_n(w)$. According to this lemma, if $g : \mathbb{C}^{d_1} \to \mathbb{C}^{d_1^*}$ is a surjective linear map defined over $\mathbb{Q}$, and if we set $U = \ker g$, then we have

$$\ell_1^* := \dim_{\mathbb{Q}} g(X) = \dim_{\mathbb{Q}}(X/(X \cap U)) \geq \dim_{\mathbb{C}}(\mathbb{C}^{d_1}/U) = d_1^*.$$

This uses the hypothesis that w does not belong to any vector subspace of $\mathbb{C}^n$ defined over $\mathbb{Q}$ and contained in W. Since $d_1 = \ell_1$, the above inequality shows that the last hypothesis of Theorem 10.1 is satisfied. Moreover, since $w \in W$, the matrix $\theta_n(w)$ has rank $r \leq N/2$. We deduce that the family (10.7) admits a measure of simultaneous approximation of the form

$$CD^{r\kappa+1}(h + \log D)^{r\kappa+1}(\log D)^{-r\kappa-1}$$

with

$$\kappa = 2/d_1 = 2^{-n+1} \quad \text{and} \quad r \leq d_1/2 = 2^{n-1} = 1/\kappa.$$

This yields the desired result. $\square$

Proof of Theorem 2.8.

Write the polynomial Q in the form

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j$$

with rational numbers $a_{11}, \ldots, a_{nn}$. Define a $\mathbb{C}$-linear map $\varphi : \mathbb{C}^n \to \mathbb{C}^{2n}$ by

$$\varphi(z_1, \ldots, z_n) = \Big(z_1, \ldots, z_n, \sum_{j=1}^n a_{1j} z_j, \ldots, \sum_{j=1}^n a_{nj} z_j\Big),$$

and consider the point $w = \varphi(\lambda_1, \ldots, \lambda_n)$. Since $(\lambda_1, \ldots, \lambda_n)$ is a zero of Q in $\mathcal{L}^n$, the point w belongs to $W \cap \mathcal{L}^{2n}$, where W is the hypersurface defined in Corollary 10.2. Let E denote the smallest vector subspace of $\mathbb{C}^n$, which is defined over $\mathbb{Q}$, and contains w. Since $\lambda_1, \ldots, \lambda_n$ are $\mathbb{Q}$-linearly independent, and since E is defined over $\mathbb{Q}$, E contains $\varphi(\mathbb{C}^n)$. Moreover, $\varphi(\mathbb{C}^n)$ is not contained in W because the polynomial Q does not vanish identically on $\mathbb{C}^n$. Hence, E is not contained in W, and the conclusion follows from Corollary 10.2 and Proposition 1.3. $\square$

Remark. One deduces Corollary 10.2 from Theorem 2.8 by considering a basis $\lambda_1, \ldots, \lambda_m$ of the $\mathbb{Q}$-vector space spanned by the $2n$ numbers $x_1, \ldots, x_n, y_1, \ldots, y_n$: from the hypothesis $w \in W$ of Corollary 10.2 we deduce that $\lambda_1, \ldots, \lambda_m$ satisfy a nontrivial homogeneous quadratic dependence relation. So, the two results are, in fact, equivalent.

§11. Proof of Theorem 4.1

Under the assumptions of Theorem 4.1, set $\alpha = \wp(\omega_1/2)$ and $\beta = \wp'(\omega_1/2)$. Let K_0 denote the number field $\mathbb{Q}(g_2, g_3, \alpha, \beta)$, and let c_0, D_0 and h_0 be positive integers. Choose algebraic numbers $\gamma_1, \gamma_2, \gamma_1', \gamma_2'$, and set

$$K = K_0(\gamma_1, \gamma_2, \gamma_1', \gamma_2'),$$

$$h = \max\{h_0, \mathrm{h}(\gamma_1), \mathrm{h}(\gamma_2), \mathrm{h}(\gamma_1'), \mathrm{h}(\gamma_2')\} \quad \text{and} \quad D = \max\{D_0, [K:\mathbb{Q}]\}.$$

We will show that the hypothesis

$$|\omega_1 - \gamma_1| + |\omega_2 - \gamma_2| + |\eta_1 - \gamma_1'| + |\eta_2 - \gamma_2'| \le \exp\{-2c_0^{14} D^{3/2}(h + \log D)^{3/2}\}$$

leads to a contradiction if c_0, D_0 and h_0 are sufficiently large, independently of the choice $\gamma_1, \gamma_2, \gamma_1', \gamma_2'$, and from this the conclusion will follow.

Let $\mathbb{E}$ be the elliptic curve over K_0 which is associated with $\wp$, and let σ be the Weierstraß sigma function associated with $\wp$. It is known that an extension G_1 of $\mathbb{E}$ by the additive group $\mathbb{G}_{\mathrm{a}}$ admits an embedding in $\mathbb{P}_5$. Explicit formulas for the exponential map of $G_1(\mathbb{C})$ are given by M. Hindry in [12]. These formulas identify the tangent space $T_{G_1}(\mathbb{C})$ with $\mathbb{C}^2$. Here, we consider the nonisotrivial extension G_1 whose exponential map $\exp_{G_1} : \mathbb{C}^2 \to G_1(\mathbb{C})$ is given by the entire functions $\varphi_0, \dots, \varphi_5$, with

$$\varphi_0(z_1, z_2) = \sigma(z_2)^3, \qquad \varphi_1/\varphi_0(z_1, z_2) = \wp(z_2), \qquad \varphi_2/\varphi_0(z_1, z_2) = \wp'(z_2),$$

$$\varphi_3/\varphi_0(z_1, z_2) = z_1 + \zeta(z_2), \qquad \varphi_4/\varphi_0(z_1, z_2) = \wp(z_2)(z_1 + \zeta(z_2)) + \frac{1}{2}\wp'(z_2),$$

$$\varphi_5/\varphi_0(z_1, z_2) = \wp'(z_2)(z_1 + \zeta(z_2)) + 2\wp^2(z_2).$$

We shall achieve the required contradiction by applying Theorem 2.1 of [33] to the product $G = \mathbb{G}_{\mathrm{a}} \times G_1$. In the notations of this theorem, we thus have $d_0 = 1$, $d_1 = 0$, $d_2 = 2$, $d = 3$, $n = 1$ and $\delta_1 = 2$. The group G is defined over K_0 and therefore is defined over K. Moreover, if we identify $T_G(\mathbb{C})$ with $\mathbb{C} \times T_{G_1}(\mathbb{C}) = \mathbb{C}^3$, then $T_G(K)$ becomes identified with K^3. We choose

$$\ell_0 = 1 \quad \text{and} \quad w_1' = w_1 = (1, 0, 1).$$

Then, $W = Kw_1$ is a subspace of $T_G(K)$ and we have $\mathcal{W}' = \mathbb{C}w_1'$. We will also take $\mathcal{V}' = \mathcal{W}'$, thus $r = r_3 = 1$ and $r_1 = r_2 = 0$. Define parameters $A, B, \dots, V$ by

$$\begin{aligned} \log A &= c_0^9(h + \log D), \\ \log B &= c_0(h + \log D), \\ T_0 = S_0 &= \left[c_0^{11} D^{1/2}(h + \log D)^{1/2}\right] \\ T_1 &= \left[c_0^3 D^{1/2}(h + \log D)^{1/2}\right] \\ S_1 &= \left[c_0^4 D^{1/2}(h + \log D)^{1/2}\right] \\ U &= c_0^{13} D^{3/2}(h + \log D)^{3/2}, \end{aligned}$$

$$A_1 = A, \qquad B_1 = B_2 = B, \qquad E = e \quad \text{and} \quad V = c_0 U.$$

It is easy to check that they satisfy all the hypotheses in §2 f) of [33]. Essentially, one verifies

$$DT_0 \log B = DS_0 \log B \leq U, \quad DT_1 \log A \leq U, \quad \text{and} \quad B \geq T_0 + T_1 + 3S_0.$$

The main condition in §2 g) of [33] which imposes bounds on the value $H(G; T_0, T_1)$ of the Hilbert function of G follows from the inequalities

$$\frac{1}{2} c_0^4 U < T_0 T_1^2 \leq c_0^4 U.$$

We put $M = S_1^2$ and we choose for $\eta_1', \ldots, \eta_M' \in \mathcal{V}'$ the following multiples of w_1'

$$\big((s_1 + 1/2)\omega_1 + s_2\omega_2,\ 0,\ (s_1 + 1/2)\omega_1 + s_2\omega_2 \big), \qquad (0 \leq s_1, s_2 < S_1).$$

Accordingly, we take

$$\Sigma = \big\{ \exp_G(\eta_1), \ldots, \exp_G(\eta_M) \big\} \subset G(K)$$

where $\eta_1, \ldots, \eta_M$ denote the points

$$\big((s_1 + 1/2)\gamma_1 + s_2\gamma_2,\ (s_1 + 1/2)(\gamma_1' - \eta_1) + s_2(\gamma_2' - \eta_2),\ (s_1 + 1/2)\omega_1 + s_2\omega_2 \big),$$

with $0 \leq s_1, s_2 < S_1$. If we compute the image of such a point under the exponential map of G, we find that its projection on the factor $\mathbb{G}_a$ is

$$(s_1 + 1/2)\gamma_1 + s_2\gamma_2,$$

and that its projection on G_1 is

$$\Big(1 \ :\ \alpha \ :\ \beta \ :\ (s_1 + 1/2)\gamma_1' + s_2\gamma_2' \\ :\ \alpha\big((s_1 + 1/2)\gamma_1' + s_2\gamma_2'\big) + \beta/2 \ :\ \beta\big((s_1 + 1/2)\gamma_1' + s_2\gamma_2'\big) + 2\alpha^2 \Big).$$

The height of this last point in $\mathbb{P}_5(K)$ is bounded above by

$$c_0(\log S_1 + h) \leq \log A.$$

Moreover, the height of the point $(1 : w_1)$ in $\mathbb{P}_3(K)$ as well as the height of the point in $\mathbb{P}_M(K)$ with projective coordinates 1 and $(s_1 + 1/2)\gamma_1 + s_2\gamma_2$, $(0 \leq s_1, s_2 < S_1)$, are both bounded above by $\log B$. Finally, for any real $R \geq 0$ and any $z \in \mathbb{C}^3$ with $|z| \leq R$, we have

$$-H^-(R) \leq \log \max\{|\varphi_0(z)|, \ldots, |\varphi_5(z)|\} \leq H^+(R)$$

with $H^-(R) = c_0$ and $H^+(R) = c_0^{1/3}R^2$. Since all the points η_j have norm $|\eta_j| \le c_0^{1/4}S_1$ and since

$$H^+(c_0^{1/3}S_1) = c_0S_1^2 \le D\log A,$$

we find that all the conditions in §2 e) of [33] are fulfilled.

Finally, our hypothesis gives $|\eta'_j - \eta_j| \le e^{-V}$ for $j = 1, \dots, M$, and we clearly have $|w'_1 - w_1| \le e^{-V}$. Therefore we can use Theorem 2.1 of [33]. It provides a connected algebraic subgroup G^* of G, distinct from G, such that, if we define

$$W^* = \big(W + T_{G^*}(K)\big)/T_{G^*}(K), \qquad \Sigma^* = \big(\Sigma + G^*(K)\big)/G^*(K),$$

$$\ell_0^* = \dim_K W^* \quad \text{and} \quad M^* = \operatorname{Card}\Sigma^*,$$

then, since $\deg G_1 = 6$ (see [12]), we have

$$S_0^{\ell_0^*}M^*\mathcal{H}(G^*; T_0, T_1) \le 72T_0T_1^2. \tag{11.1}$$

Since G^* is a proper subgroup of G, it must be contained either in $\{0\} \times G_1$ or in the subgroup L of G whose tangent space inside $T_G(\mathbb{C}) = \mathbb{C}^3$ is $\mathbb{C}^2 \times \{0\}$. This group L is isomorphic to $\mathbb{G}_{\mathrm{a}}^2$ and yields a quotient G/L isomorphic to $\mathbb{E}$. Since w_1 does not belong to $\{0\} \times \mathbb{C}^2$ nor to $\mathbb{C}^2 \times \{0\}$, we must have $\ell_0^* = 1$ in all cases. If G^* is contained in L and has dimension 2, we find

$$M^* = 1 \quad \text{and} \quad \mathcal{H}(G^*; T_0, T_1) \ge 2T_0T_1.$$

If G^* is contained in L and has dimension 1, its tangent space cannot contain both $(\gamma_1, \gamma'_1, 0)$ and $(\gamma_2, \gamma'_2, 0)$ because the determinant $\gamma_1\gamma'_2 - \gamma_2\gamma'_1$ is close to $\omega_1\eta_2 - \omega_2\eta_1$ which itself is equal to $\pm 2i\pi$ by virtue of Legendre's relation. Since every η_j is congruent modulo the group of periods of G to a point of the form

$$\eta + s_1(\gamma_1, \gamma'_1, 0) + s_2(\gamma_2, \gamma'_2, 0)$$

for some fixed $\eta \in \mathbb{C}^3$, we deduce that, in that case, we have

$$M^* \ge S_1 \quad \text{and} \quad \mathcal{H}(G^*; T_0, T_1) \ge \min\{T_0, T_1\} = T_1.$$

Finally, if G^* is contained in $\{0\} \times G_1$ or if it has dimension 0, its tangent space contains no linear combination of $(\gamma_1, \gamma'_1, 0)$ and $(\gamma_2, \gamma'_2, 0)$, and so the above argument gives

$$M^* = S_1^2 \quad \text{and} \quad \mathcal{H}(G^*; T_0, T_1) \ge 1.$$

Since $T_0 \ge S_1 \ge T_1$, we thus have, in all three cases, $M^*\mathcal{H}(G^*; T_0, T_1) \ge S_1T_1$ and (11.1) yields

$$S_0S_1T_1 \le 72T_0T_1^2.$$

Since $S_0 = T_0$ and $S_1 > (c_0/2)T_1$, this is the desired contradiction. ∎

References

[1] Baker, A.: *Transcendental Number Theory;* Cambridge Univ. Press, 2nd ed. 1979.

[2] Barré-Sirieix K., Diaz G., Gramain F., et Philibert G.: Une preuve de la conjecture de Mahler-Manin; Invent. Math., **124** (1996), 1–9.

[3] Bertrand, D., Philippon P.: Sous-groupes algébriques de groupes algébriques commutatifs; Illinois J. Math., **32** (1988), 263–280.

[4] Brownawell, W.D.: The algebraic independence of the values of the exponential function; K. Norske Vidensk. Selsk. Skr., **23** (1972), 5 pp.

[5] Brownawell, W.D.: Sequences of Diophantine Approximations; J. Number Theory **6** (1974), 11–21.

[6] Chudnovsky, G.V.: *Contributions to the theory of transcendental numbers*; Math. Surveys and Monographs, n°19, A.M.S. (1984).

[7] Chudnovsky, G.V.: Algebraic independence of the values of elliptic functions at algebraic points; Invent. Math., **61** (1980), 267–290.

[8] Diaz, G.: Une nouvelle minoration de $|\log\alpha-\beta|$, $|\alpha-\exp\beta|$, α et β algébriques; Acta Arith., 64 (1993), 43–57; compléments: Séminaire d'Arithmétique Univ. St. Etienne 1990–91–92, N°4, 49–58.

[9] Feldman, N.I.: *Hilbert's seventh problem*; Moscow, Moscow State University, 1982, 311 pp.

[10] Forster, O.: *Lectures on Riemann surfaces*; Graduate Texts in Math., **81**, Springer–Verlag (1981), 254 pp.

[11] Gel'fond, A.O.: *Transcendental and algebraic numbers;* Moscow, 1952; Engl. transl., Dover Publ., N.Y., 1960.

[12] Hindry, M.: Groupes algébriques commutatifs, exemples explicites, in: Séminaire d'Arithmétique Saint-Etienne 1988–89, exposé no. 2, 34pp.

[13] Lang, S.: *Introduction to transcendental numbers;* Addison Wesley, 1966.

[14] Masser, D., and Wüstholz, G.: Algebraic independence properties of values of elliptic functions; in *Journées arithmétiques* 1980, Ed. J.V. Armitage, London Math. Soc. Lect. Note Ser. **56** (1982), 360–363.

[15] Masser, D., and Wüstholz, G.: Fields of large transcendence degree generated by values of elliptic functions; Invent. Math., **72** (1983), 407–464.

[16] Mignotte, M., et Waldschmidt, M.: Approximation simultanée de valeurs de la fonction exponentielle ; Compositio Math., **34** (1977), 127–139.

[17] Nesterenko, Yu.V.: Modular functions and transcendence problems, C. R. Acad. Sc. Paris, Sér. 1 **322** (1996), 909–914; Math. Sb., **187** N° 9 (1996), 65–96.

[18] Nesterenko, Yu.V., and Waldschmidt, M.: On the approximation of the values of exponential function and logarithm by algebraic numbers; Russian Math. Transactions, Moscow, **2** (1996), 23–42.

[19] Philippon, P.: Une approche méthodique pour la transcendance et l'indépendance algébrique de valeurs de fonctions analytiques; J. Number Theory, **64** (1997), 291–338.

[20] Roy, D., and Waldschmidt, M.: Quadratic relations between logarithms of algebraic numbers; Proc. Japan Acad. Sci., Sér. A, **71** (1995), 151–153.

[21] Roy, D., and Waldschmidt, M.: Approximation diophantienne et indépendance algébrique de logarithmes; Ann. Sci. École Norm. Sup., (to appear).

[22] Shorey, T.N.: On the sum $\sum_{k=1}^{3} |2^{\pi^k} - \alpha_k|$, α_k algebraic numbers; J. Number Theory, **6** (1974), 248–260.

[23] Srinivasan, S.: On algebraic approximations to 2^{π^k}, $(k = 1, 2, 3, \ldots)$; Indian J. Pure Appl. Math., **5** (1974), 513–523; (II), J. Indian Math. Soc., **43** (1979), 53–60.

[24] Tijdeman, R.: On the algebraic independence of certain numbers; Proc. Nederl. Akad. Wetensch., Ser. A, **74** (= Indag. Math., **33**) (1971), 146–162.

[25] Tubbs, R.: Elliptic curves in two dimensional abelian varieties and the algebraic independence of certain numbers; Michigan Math. J., **34** (1987), 173–182.

[26] Tubbs, R.: Algebraic groups and small transcendence degree, I ; J. Number Theory **25** (1987), 279–307; II; id., **35** (1990), 109–127.

[27] Vaaler, J.: A Geometric inequality with applications to linear forms; Pacific J. Math. **83** (1979), 543–553.

[28] Waldschmidt, M.: *Nombres transcendants ;* Lecture Notes in Math., **402**, Springer–Verlag (1974), 277 pp.

[29] Waldschmidt, M.: Transcendence measures for numbers connected with the exponential function; J. Austral. Math. Soc., **25** (1978), 445–465.

[30] Waldschmidt, M.: Transcendance et exponentielles en plusieurs variables; Invent. Math., **63** (1981), 97–127.

[31] Waldschmidt, M.: Algebraic independence of transcendental numbers — Gel'fond's method and its developments ; Perspective in Mathematics (Anniversary of Oberwolfach 1984), Birkhäuser Verlag (1984), 551–571.

[32] Waldschmidt, M.: *Linear independence of logarithms of algebraic numbers ;* The Institute of Mathematical Sciences, Madras, IMSc Report No **116**, (1992), 168 pp.

[33] Waldschmidt, M.: Approximation diophantienne dans les groupes algébriques commutatifs; J. reine angew. Math., (to appear).

[34] Wirsing, E.: Approximation mit algebraischen Zahlen beschränkten Grades; J. reine angew. Math., **206** (1961), 67-77.

Damien ROY
Département de mathématiques
Université d'Ottawa
585 King Edward
Ottawa, Ontario K1N 6N5, CANADA

Michel WALDSCHMIDT
Institut de Mathématiques de Jussieu
Case 247 Problèmes Diophantiens
4, Place Jussieu
75252 PARIS Cedex 05 FRANCE

Typeset: June 22 1998 at 11h15.