Fields' off-site summer school at the University of Ottawa
Analytic Number Theory and Diophantine Approximation, June 30 – July 11, 2008

Application to Gel'fond's Problem

Lecture 5

Damien Roy (*University of Ottawa*)

This last lecture is inspired by a survey of Michel Waldschmidt on large transcendence degrees [7]. Its goal is to show on a concrete example how Philippon's criterion can be combined with a zero estimate to prove results of algebraic independence. To this end, consider the following conjecture known as Gel'fond's problem.

Conjecture. Let $\alpha \in \mathbb{C}$ be a non-zero algebraic number and let $\beta \in \mathbb{C}$ be an irrational algebraic number. Denote by d the degree of β over $\mathbb{Q}$ and choose a non-zero determination $\log(\alpha)$ of the logarithm of α. Then, the $d-1$ complex numbers

$$\alpha^{\beta^j} := \exp(\beta^j \log(\alpha)), \quad j = 1, \dots, d-1,$$

are algebraically independent over $\mathbb{Q}$.

Under the hypotheses of this conjecture, the well-known theorem of Gel'fond and Schneider asserts that α^β is transcendental. So, the conjecture is true when $d = 2$. In 1949, Gel'fond also proved that the conjecture holds when $d = 3$ [2]. For any larger value of d, it is still open. However, we possess general lower bounds for the transcendence of the field generated by these numbers:

$$\begin{aligned} \operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}\big(\alpha^\beta, \dots, \alpha^{\beta^{d-1}}\big) \;&\geq\; \log_2(d/2) \quad &&\text{Chudnovsky 1976,} \\ &\geq\; (d-1)/2 &&\text{Philippon 1987,} \\ &\geq\; d/2 &&\text{Diaz 1989.} \end{aligned}$$

We will show here that this transcendence degree is at least $(d-2)/4$ when α and β are real with $\alpha > 0$ and $\log(\alpha) \in \mathbb{R}$ (we restrict to real numbers in order to avoid technicalities in the application of the zero estimate).

1. Technical hypotheses

To recast the above results in a larger context, we need the following concept.

Definition. Let $\xi_0, \dots, \xi_n$ be $\mathbb{Q}$-linearly independent complex numbers. We say that $\xi_0, \dots, \xi_n$ satisfy the *Technical Hypothesis* (`T.H.`) if, for each $\epsilon > 0$, there exist only finitely many integers H for which the conditions

$$0 < \max\{|m_0|, \dots, |m_n|\} \leq H, \quad |m_0\xi_0 + \cdots + m_n\xi_n| \leq \exp(-H^\epsilon)$$

admit a solution $(m_0, \dots, m_n) \in \mathbb{Z}^n$.

For example, upon denoting by $\bar{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, we have:

Lemma 1.1. *Let* $1, \beta_1, \dots, \beta_n \in \bar{\mathbb{Q}}$ *be* $\mathbb{Q}$*-linearly independent, and let* $\xi \in \mathbb{C}^\times$*. Then* $\xi, \xi\beta_1, \dots, \xi\beta_n$ *satisfy T. H.*

Proof. Without loss of generality, we may assume that $\xi = 1$. Let W denote the smallest $\mathbb{Q}$-subvariety of $\mathbb{P}_n(\mathbb{C})$ containing the point with projective coordinates $(1, \beta_1, \dots, \beta_n)$. Over $\bar{\mathbb{Q}}$, its Chow form factors as a product

$$F = a \prod_{i=1}^{d} \left(U_0 + \beta_1^{(i)} U_1 + \cdots + \beta_n^{(i)} U_n \right) \in \mathbb{Z}[U_0, \dots, U_n]$$

where $(\beta_1^{(i)}, \dots, \beta_n^{(i)})$ $(i = 1, \dots, d)$ are the distinct conjugates of $(\beta_1, \dots, \beta_n)$ over $\mathbb{Q}$ and where $a \in \mathbb{Z} \setminus \{0\}$. For any non-zero point $\mathbf{m} = (m_0, \dots, m_n) \in \mathbb{Z}^{m+1}$, the value $F(\mathbf{m})$ is a non-zero integer with

$$|F(\mathbf{m})| \le c \, \|\mathbf{m}\|^{d-1} |m_0 + m_1\beta_1 + \cdots + m_n\beta_n|$$

for some constant $c > 0$ depending only on W, and so $|m_0 + m_1\beta_1 + \cdots + m_n\beta_n| \ge c^{-1} \|\mathbf{m}\|^{-d+1}$. The conclusion follows. □

In [1], G. Diaz proved the following result:

Theorem 1.2 (Diaz, 1989)**.** *Let* $x_1, \dots, x_d \in \mathbb{C}$ *be* $\mathbb{Q}$*-linearly independent numbers satisfying T. H., and let* $y_1, \dots, y_\ell \in \mathbb{C}$ *be* $\mathbb{Q}$*-linearly independent numbers satisfying also T. H. Assume that* $d\ell > d + \ell$*. Then we have*

$$\mathrm{trdeg}_{\mathbb{Q}} \mathbb{Q}(x_1, \dots, x_d, e^{x_1 y_1}, \dots, e^{x_d y_\ell}) > \frac{(d-1)\ell}{d+\ell} \cdot$$

The earlier result [3, Thm. 2.12] of P. Philippon had a large inequality instead of the strict inequality. So, the above is an improvement when $d + \ell$ divides $(d-1)\ell$. It is conjectured that this result still holds without any technical hypotheses (see [7, §2]). In the notation of Gel'fond's problem, Lemma 1.1 shows that the hypotheses of Diaz' theorem are satisfied with $\ell = d$ and $x_j = \beta^{j-1}$, $y_j = \beta^{j-1} \log(\alpha)$ for $j = 1, \dots, d$. This gives

$$\frac{d-1}{2} < \mathrm{trdeg}_{\mathbb{Q}} \mathbb{Q}(1, \beta, \dots, \beta^{d-1}, \alpha, \alpha^{\beta}, \dots, \alpha^{\beta^{2d-2}}) = \mathrm{trdeg}_{\mathbb{Q}} \mathbb{Q}(\alpha^{\beta}, \dots, \alpha^{\beta^{d-1}}),$$

and, since the above transcendence degree is an integer, it is $\ge d/2$, as stated in the presentation. In this lecture, we will simply prove:

Proposition 1.3. *Let* $x_1, \dots, x_d \in \mathbb{R}$ *be* $\mathbb{Q}$*-linearly independent numbers satisfying T. H., and let* $y_1, \dots, y_\ell \in \mathbb{R}$ *be* $\mathbb{Q}$*-linearly independent numbers satisfying also T. H. Assume that* $d\ell > d + \ell$*. Then we have*

$$\mathrm{trdeg}_{\mathbb{Q}} \mathbb{Q}(e^{x_1 y_1}, \dots, e^{x_d y_\ell}) \ge \frac{d\ell - d - \ell}{2(d+\ell)} \cdot$$

Arguing as above, this gives $\mathrm{trdeg}_{\mathbb{Q}} \mathbb{Q}(\alpha^{\beta}, \dots, \alpha^{\beta^{d-1}}) \ge (d-2)/4$ in the notation of Gel'fond's problem, assuming that $\log(\alpha)$ and β are real.

2. Proof of Proposition 1.3

We proceed in several steps. The first one is a special case of a construction of Michel Waldschmidt whose proof in presented in Appendix B.

Step 1. Let α, β, ρ and ν be positive real numbers with

$$\beta \le \nu, \quad \alpha + \rho < \nu \quad \text{and} \quad 2\nu < d\alpha + \beta. \tag{1}$$

For each sufficiently large integer N, there exists a non-zero polynomial $P_N \in \mathbb{Z}[X_1, \dots, X_n]$ with

$$\deg(P_N) \le N^\alpha, \quad \log \|P_N\| \le N^\beta,$$

such that the exponential polynomial $f_N(z) := P_N(e^{x_1 z}, \dots, e^{x_d z})$ satisfies

$$|f_N|_{N^\rho} := \max\{|f_N(z)|\,;\, |z| \le N^\rho\} \le \exp(-N^\nu).$$

Step 2. Fix a real number σ with

$$0 < \sigma < \rho. \tag{2}$$

For each sufficiently large integer N and each $\mathbf{s} = (s_1, \dots, s_\ell) \in \mathbb{N}^\ell$ with $\|\mathbf{s}\| \le N^\sigma$, we have

$$|s_1 y_1 + \cdots + s_\ell y_\ell| \le N^\rho,$$

and so

$$|f_N(s_1 y_1 + \cdots + s_\ell y_\ell)| \le \exp(-N^\nu).$$

Upon writing

$$\underline{\gamma}_j = (e^{x_1 y_j}, \dots, e^{x_d y_j}) \in \mathbb{T} := (\mathbb{C}^\times)^d \quad \text{for } j = 1, \dots, \ell,$$

where $\mathbb{T}$ is the algebraic group considered in Lectures 1-2 (for the field $K = \mathbb{C}$), the preceding inequality becomes

$$|P_N(\underline{\gamma}_1^{s_1} \cdots \underline{\gamma}_\ell^{s_\ell})| \le \exp(-N^\nu).$$

In particular, if $\mathbf{s} = 0$, this implies that $P_N(\mathbf{1}) = 0$, where $\mathbf{1}$ denotes the neutral element of $\mathbb{T}$, because $P_N(\mathbf{1}) \in \mathbb{Z}$. Furthermore upon writing

$$P_N(X_1, \dots, X_d) = \sum_{|\underline{\lambda}| \le N^\alpha} p_{N,\underline{\lambda}} X_1^{\lambda_1} \cdots X_d^{\lambda_d},$$

we find that

$$P_N(\underline{\gamma}_1^{s_1} \cdots \underline{\gamma}_\ell^{s_\ell}) = Q_N^{(\mathbf{s})}\big(1, \underline{\gamma}_1, \dots, \underline{\gamma}_\ell\big)$$

where $Q_N^{(\mathbf{s})}$ is the homogeneous polynomial of

$$\mathbb{Z}[Y_0, \mathbf{Y}_1, \dots, \mathbf{Y}_\ell], \quad \mathbf{Y}_j = (Y_{1,j}, \dots, Y_{d,j}) \quad j = 1, \dots, \ell,$$

of degree $D_N := [\ell N^{\alpha+\sigma}]$ given by

$$Q_N^{(\mathbf{s})}\big(Y_0, \mathbf{Y}_1, \dots, \mathbf{Y}_\ell\big) = \sum_{|\underline{\lambda}| \le N^\alpha} p_{N,\underline{\lambda}} Y_0^{D_N - |\underline{\lambda}|\,|\mathbf{s}|} \prod_{i=1}^{d} \prod_{j=1}^{\ell} Y_{i,j}^{\lambda_i s_j}$$

We also note that $\|Q_N^{(\mathbf{s})}\| = \|P_N\|$ if $\mathbf{s} \neq 0$. Since $Q_N^{(0)} = P_N(\mathbf{1})Y_0^{D_N} = 0$, we conclude that $\|Q_N^{(\mathbf{s})}\| \leq \exp(N^\beta)$ regardless whether $\mathbf{s}$ is zero or not.

Consider the family $\mathcal{F}_N$ of all polynomials $Q_N^{(\mathbf{s})}$ with $\mathbf{s} \in \mathbb{N}^\ell$ of norm $\|\mathbf{s}\| \leq N^\sigma$. By construction, each $Q \in \mathcal{F}_N$ is homogeneous of degree $D_N = [\ell N^{\alpha+\sigma}]$ and satisfies

$$\log \|Q\| \leq N^\beta \quad \text{and} \quad |Q(1, \underline{\gamma}_1, \ldots, \underline{\gamma}_\ell)| \leq \exp(-N^\nu).$$

Moreover, a common zero of this family in $\mathbb{P}_{d\ell}(\mathbb{C})$ with non-zero first projective coordinate is represented by a point $(1, \underline{\tilde{\gamma}}_1, \ldots, \underline{\tilde{\gamma}}_\ell) \in \mathbb{C}^{1+d\ell}$ with the property that

$$P_N(\underline{\tilde{\gamma}}_1^{s_1} \cdots \underline{\tilde{\gamma}}_\ell^{s_\ell}) = 0 \quad \text{for any } \mathbf{s} \in \mathbb{N}^\ell \text{ with } \|\mathbf{s}\| \leq N^\sigma. \tag{3}$$

This last remark will be useful later.

In order to conclude on the basis of Philippon's criterion that

$$\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\underline{\gamma}_1, \ldots, \underline{\gamma}_\ell) \geq k + 1,$$

for some integer $k \geq 0$, we require that

$$\nu > \max\{\beta,\, \alpha + \sigma\} + k(\alpha + \sigma) \tag{4}$$

so that the ratio $N^\nu / \big((N^\beta + D_N) D_N^k\big)$ tends to 0 as N goes to infinity. We also require that the family $\mathcal{F}_N$ has no common zero at distance $\leq \exp(-(N-1)^\nu)$ from the point θ of $\mathbb{P}_{d\ell}(\mathbb{C})$ with projective coordinates $(1, \underline{\gamma}_1, \ldots, \underline{\gamma}_\ell)$.

Step 3. Suppose that the family $\mathcal{F}_N$ has a common zero $\tilde{\theta}$ at a distance $\leq \exp(-(N-1)^\nu)$ from θ. Since θ is independent of N, this implies, if N is large enough, that $\tilde{\theta}$ admits a set of projective coordinates of the form $(1, \underline{\tilde{\gamma}}_1, \ldots, \underline{\tilde{\gamma}}_\ell) \in \mathbb{C}^{1+d\ell}$ with

$$\|\underline{\tilde{\gamma}}_j - \underline{\gamma}_j\| \leq c_1 \exp(-(N-1)^\nu) \quad \text{for } j = 1, \ldots, \ell,$$

where c_1 is a positive constant depending only on θ. In turn this implies that, for each $j = 1, \ldots, \ell$, we can write

$$\underline{\tilde{\gamma}}_j = (e^{t_{1,j}}, \ldots, e^{t_{d,j}})$$

for a choice of complex numbers $t_{i,j}$ with

$$|t_{i,j} - x_i y_j| \leq c_2 \exp(-(N-1)^\nu) \tag{5}$$

for a constant $c_2 > 0$ which does not depend on N. Moreover, the points $\underline{\tilde{\gamma}}_1, \ldots, \underline{\tilde{\gamma}}_\ell$ satisfy the condition (3).

Now suppose that there exists $\mathbf{m} = (m_1, \ldots, m_d) \in \mathbb{N}^d$ with $0 < |\mathbf{m}| \leq N^\alpha$ and $\mathbf{s} = (s_1, \ldots, s_\ell) \in \mathbb{N}^\ell$ with $0 < \|\mathbf{s}\| \leq N^\sigma$ such that

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} (e^{t_{i,j}})^{m_i s_j} \;=\; 1.$$

Then the real part of $\sum_{i=1}^{d}\sum_{j=1}^{\ell} t_{i,j}m_i s_j$ is 0 and thus, by (5), we find

$$\left|\sum_{i=1}^{d}\sum_{j=1}^{\ell}(x_iy_j)m_is_j\right| = \left|\sum_{i=1}^{d}\sum_{j=1}^{\ell}\Re(t_{i,j}-x_iy_j)m_is_j\right| \le c_2\ell N^{\alpha+\sigma}\exp(-(N-1)^{\nu}),$$

where $\Re$ denotes the function "real part". Since

$$\sum_{i=1}^{d}\sum_{j=1}^{\ell}(x_iy_j)m_is_j = \left(\sum_{i=1}^{d} m_ix_i\right)\left(\sum_{j=1}^{\ell} s_jy_j\right),$$

and since both $x_1,\dots,x_d$ and $y_1,\dots,y_\ell$ satisfy T. H., this is possible only for finitely many values of N. Therefore, assuming that N is large enough, Proposition 4.1 of Lectures 1-2 applies with $D=[N^\alpha]$ and $S=[N^\sigma]$: it gives

$$\bigl(2[N^\alpha]\bigr)^d \ge \bigl([N^\sigma]/d\bigr)^\ell.$$

The existence of the zero $\tilde\theta$ is therefore ruled out, for N sufficiently large, if we assume that

$$(6)\qquad d\alpha < \ell\sigma.$$

Step 4. For any ϵ with $0<3\epsilon<d\ell+d+\ell$, the conditions (1), (2), (4) and (6) are fulfilled with

$$\alpha=\ell,\quad \sigma=d+\epsilon,\quad \rho=d+2\epsilon,\quad \beta=d+\ell+2\epsilon,\quad \nu=(d\ell+d+\ell+\epsilon)/2$$

upon taking for k the largest integer with

$$k+1<\frac{\nu-\epsilon}{d+\ell+\epsilon}\cdot$$

For such a choice of parameters, we have

$$\operatorname{trdeg}_{\mathbb{Q}}\mathbb{Q}(\underline{\gamma}_1,\dots,\underline{\gamma}_\ell)\ge k+1\ge\frac{\nu-\epsilon}{d+\ell+\epsilon}-1=\frac{d\ell-d-\ell-3\epsilon}{2(d+\ell+\epsilon)}\cdot$$

The conclusion follows by letting ϵ tend to zero.

Appendix A. The Thue-Siegel lemma

The use of the box principle for the construction of an auxiliary polynomial first appeared in the work of Thue in 1904. In 1929, in his study of integral points on algebraic curves, Siegel used it extensively and stated it as a separate lemma. We first prove a version of that lemma.

Lemma A.1 (Thue-Siegel)**.** *Let $m,\ n\in\mathbb{N}$ with $1\le m<n$, let $a_{i,j}$ $(1\le i\le m,\ 1\le j\le n)$ be real numbers, let $A>0$ be an upper bound for their absolute values, and let $\delta>0$ be any positive real number. Then the system of inequalities*

$$\begin{cases} |a_{1,1}x_1+\cdots+a_{1,n}x_n| & < \delta \\ \qquad\vdots & \\ |a_{m,1}x_1+\cdots+a_{m,n}x_n| & < \delta \end{cases}$$

admits a non-zero solution $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$ *with*

$$\|\mathbf{x}\| < 1 + \left(\frac{nA}{\delta}\right)^{\frac{m}{n-m}}.$$

The proof below is an adaptation of the argument of Siegel in [5, Lemma 1, §2, Chap. II].

Proof. Put $X = 1 + \big(nA/\delta\big)^{m/(n-m)}$ and consider the linear map $T\colon \mathbb{R}^n \to \mathbb{R}^m$ given by

$$T(x_1, \dots, x_n) = \big(a_{1,1}x_1 + \cdots + a_{1,n}x_n\,,\ \dots\ ,\ a_{m,1}x_1 + \cdots + a_{m,n}x_n\big).$$

We need to show the existence of a point $\mathbf{x} \in \mathbb{Z}^n$ with

$$1 \le \|\mathbf{x}\| < X \quad \text{and} \quad \|T(\mathbf{x})\| < \delta.$$

To this end, denote by H the largest integer with $H < X$ and form the set

$$E = \{(x_1, \dots, x_n) \in \mathbb{Z}^n\,;\, 0 \le x_j \le H \text{ for } j = 1, \dots, n\}.$$

For each $\mathbf{x} = (x_1, \dots, x_n) \in E$ and each $i = 1, \dots, m$, we have

$$B_i^- H \le a_{i,1}x_1 + \cdots + a_{i,n}x_n \le B_i^+ H,$$

where B_i^- stands for the sum of the negative coefficients among $a_{i,1}, \dots, a_{i,n}$, while B_i^+ stands for the sum of the positive coefficients. Since the interval $[B_i^- H,\, B_i^+ H]$ is independent of $\mathbf{x}$ and has length $(B_i^+ - B_i^-)H \le nAH$, it is covered by a family $\mathcal{F}_i$ of at most $1 + nAH/\delta$ open intervals of length δ. Then, each $\mathbf{x} \in E$ is mapped by T to an open cube of side length δ of the form $J_1 \times \cdots \times J_m$ with $J_i \in \mathcal{F}_i$ for $i = 1, \dots, m$.

Since E has cardinality $(H+1)^n$ and since $H + 1 \ge X$, we find

$$|E| \ge (H+1)^m X^{n-m} > (H+1)^m \max\left\{1,\, \frac{nA}{\delta}\right\}^m \ge \left(1 + \frac{nAH}{\delta}\right)^m \ge |\mathcal{F}_1| \cdots |\mathcal{F}_m|,$$

and so there exist at least two distinct points $\mathbf{x}'$ and $\mathbf{x}''$ of E whose images under T belong to the same cube $J_1 \times \cdots \times J_m$. Their difference $\mathbf{x} = \mathbf{x}' - \mathbf{x}''$ is a non-zero point with $\|\mathbf{x}\| \le H < X$ and $\|T(\mathbf{x})\| = \|T(\mathbf{x}') - T(\mathbf{x}'')\| < \delta$ as announced. □

As a corollary, we recover the statement of [5, Lemma 1, §2, Chap. II].

Corollary A.2. *Let* $m, n \in \mathbb{N}$ *with* $1 \le m < n$, *let* $a_{i,j}$ $(1 \le i \le m,\ 1 \le j \le n)$ *be integers, and let* $A > 0$ *be an upper bound for their absolute values. Then the system of equations*

$$\begin{cases} |a_{1,1}x_1 + \cdots + a_{1,n}x_n| &= 0 \\ \quad\vdots & \\ |a_{m,1}x_1 + \cdots + a_{m,n}x_n| &= 0 \end{cases}$$

admits a non-zero solution $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$ *with* $\|\mathbf{x}\| < 1 + (nA)^{m/(n-m)}$.

Proof. This follows from the above lemma by taking $\delta = 1$, upon observing that for any $(x_1, \dots, x_n) \in \mathbb{Z}^n$ the expressions $a_{i,1}x_1 + \cdots + a_{i,n}x_n$ $(i = 1, \dots, m)$ are integers and so they are zero if their absolute values are < 1. □

Appendix B. Construction of an auxiliary function

In real analysis, it is shown that the function $f(x) = e^x$ is given by the series $e^x = \sum_{k=0}^{\infty} x^k/k!$ converging for all $x \in \mathbb{R}$. This function is extended to the whole complex plane by putting

$$e^z = \sum_{k=0}^{\infty} \frac{z^k}{k!} \quad \text{for all } z \in \mathbb{C}.$$

The ratio test (also called d'Alembert's test) shows indeed that this series is absolutely convergent for each $z \in \mathbb{C}$. On the basis of this definition, simple manipulations of series show that

$$e^{z+w} = e^z\, e^w \quad \text{for all } z, w \in \mathbb{C}.$$

In other words, e^z provides a group homomorphism from the additive group of complex numbers $(\mathbb{C}, +)$ to its multiplicative group $(\mathbb{C}^\times, \cdot)$, where $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ (we have $e^z \cdot e^{-z} = e^0 = 1$ and so e^z is non-zero with inverse e^{-z}). In particular, we have $e^{mz} = (e^z)^m$ for any $m \in \mathbb{Z}$.

The convergence of the exponential series on the whole of $\mathbb{C}$ comes from the fact that $k!$ grows to infinity faster than any geometric sequence r^k with fixed ratio $r > 1$. More precisely, for any integer $K \geq 1$, we have

$$e^K = \sum_{k=0}^{\infty} \frac{K^k}{k!} \geq \frac{K^K}{K!} \quad \Longrightarrow \quad K! \geq \left(\frac{K}{e}\right)^K.$$

Using this, we can estimate the tail of the exponential series truncated at the order K:

$$\left| \sum_{k=K}^{\infty} \frac{z^k}{k!} \right| \leq \sum_{k=K}^{\infty} \frac{|z|^k}{(k/e)^k} \leq \sum_{k=K}^{\infty} \left(\frac{e|z|}{K}\right)^k.$$

In particular, if we assume that $|z| \leq e^{-2}K$, this gives

$$\left| \sum_{k=K}^{\infty} \frac{z^k}{k!} \right| \leq \sum_{k=K}^{\infty} e^{-k} \leq 2e^{-K}.$$

The next proposition combines the Thue-Siegel lemma together with estimates of the above type to produce a so-called *auxiliary function*: an analytic function (here an exponential polynomial) taking small values in a large disk of $\mathbb{C}$ (in general of $\mathbb{C}^n$). It is a very special case of a general construction of Michel Waldschmidt in [6]. The proof given below avoids the use of the Schwarz lemma, and stresses the importance of the factorials appearing in the coefficients of the exponential series.

Proposition B.1. *Let $d \in \mathbb{N}^*$, let $x_1, \ldots, x_d \in \mathbb{C}$, and let α, β, ρ and ν be positive real numbers with*

$$\beta \leq \nu, \quad \alpha + \rho < \nu \quad \text{and} \quad 2\nu < d\alpha + \beta.$$

For each sufficiently large integer N, there exists a non-zero polynomial $P_N \in \mathbb{Z}[X_1, \dots, X_d]$ with

$$\deg(P_N) \le N^\alpha, \quad \log \|P_N\| \le N^\beta,$$

such that the exponential polynomial $f_N(z) := P_N(e^{x_1 z}, \dots, e^{x_d z})$ satisfies

$$|f_N|_{N^\rho} := \max\{|f_N(z)|\,;\ |z| \le N^\rho\} \le \exp(-N^\nu).$$

Proof. We first note that the hypotheses on the parameters imply that $\nu < d\alpha + \beta - \nu \le d\alpha$. We will use this below.

Fix an integer $N \ge 1$ and, for simplicity, put

$$D = [N^\alpha], \quad r = N^\rho, \quad V = N^\nu \quad \text{and} \quad K = [3V].$$

A general polynomial $P \in \mathbb{Z}[X_1, \dots, X_d]$ of degree $\le D$ takes the form

$$P = \sum_{|\underline{\lambda}| \le D} p_{\underline{\lambda}} \mathbf{X}^{\underline{\lambda}}$$

with unknown integral coefficients $p_{\underline{\lambda}}$. The corresponding exponential polynomial is

$$f(z) = \sum_{|\underline{\lambda}| \le D} p_{\underline{\lambda}} \exp((\underline{\lambda} \cdot \mathbf{x}) z) = \sum_{k=0}^{\infty} \left(\sum_{|\underline{\lambda}| \le D} p_{\underline{\lambda}} \frac{(\underline{\lambda} \cdot \mathbf{x})^k}{k!} \right) z^k,$$

where $\underline{\lambda} \cdot \mathbf{x} = \lambda_1 x_1 + \cdots + \lambda_d x_d$. To control its modulus $|f|_r$ on the disk of radius r centered at the origin, we use

$$|f|_r \le \sum_{k=0}^{K-1} \left| \sum_{|\underline{\lambda}| \le D} p_{\underline{\lambda}} \frac{(\underline{\lambda} \cdot \mathbf{x})^k r^k}{k!} \right| + \|P\| \sum_{k=K}^{\infty} \sum_{|\underline{\lambda}| \le D} \frac{|\underline{\lambda} \cdot \mathbf{x}|^k r^k}{k!}, \tag{7}$$

and first require that

$$\left| \sum_{|\underline{\lambda}| \le D} p_{\underline{\lambda}} \frac{(\underline{\lambda} \cdot \mathbf{x})^k r^k}{k!} \right| \le \exp(-2V) \quad \text{for } k = 0, \dots, K-1. \tag{8}$$

As this is a system of linear inequations with complex coefficients, we cannot apply our version of Thue-Siegel's lemma directly to it. So we separate the real and imaginary parts of the linear forms and ask for the stronger inequalities:

$$\left| \sum_{|\underline{\lambda}| \le D} p_{\underline{\lambda}} \frac{\Re((\underline{\lambda} \cdot \mathbf{x})^k) r^k}{k!} \right| \le \frac{1}{2} \exp(-2V) \quad \text{and} \quad \left| \sum_{|\underline{\lambda}| \le D} p_{\underline{\lambda}} \frac{\Im((\underline{\lambda} \cdot \mathbf{x})^k) r^k}{k!} \right| \le \frac{1}{2} \exp(-2V)$$

for $k = 0, \dots, K-1$. Now, this represents a system of $m := 2K$ linear inequations with real coefficients in the $n := \binom{D+d}{d}$ unknown coefficients of P. The coefficients of this system have absolute value at most

$$\max_{|\underline{\lambda}| \le D} \frac{|\underline{\lambda} \cdot \mathbf{x}|^k r^k}{k!} \le \frac{(c_1 D r)^k}{k!} \le \exp(c_1 D r) \quad \text{where } c_1 = \max\{|x_1|, \dots, |x_d|\}.$$

Assuming that N is sufficiently large, we also have $n \geq N^{d\alpha}/d! \geq 4m$ since $d\alpha > \nu$. Then, the Thue-Siegel lemma A.1 ensures the existence of integers $p_{\underline{\lambda}}$ not all zero with

$$\max |p_{\underline{\lambda}}| \leq 1 + \left(\frac{n \exp(c_1 Dr)}{(1/2)\exp(-2V)} \right)^{m/(n-m)} \leq 1 + \left(\frac{2n \exp(c_1 Dr)}{\exp(-2V)} \right)^{4m/(3n)}.$$

Since $\alpha + \rho < \nu$, we also have $2n \exp(c_1 Dr) \leq \exp(V)$ if N is large enough, and so

$$\|P\| = \max |p_{\underline{\lambda}}| \leq 1 + \exp(3V)^{4m/(3n)}.$$

Finally, using $2\nu < d\alpha + \beta$, we conclude that

$$\|P\| \leq \exp(N^\beta)$$

if N is sufficiently large. Combining this upper bound for $\|P\|$ with (8), the estimate (7) becomes

$$|f|_r \leq K \exp(-2V) + \exp(N^\beta) \sum_{k=K}^{\infty} \sum_{|\underline{\lambda}| \leq D} \frac{|\underline{\lambda} \cdot \mathbf{x}|^k r^k}{k!} \tag{9}$$

To estimate the series over k, we use the inequality $k! \geq (k/e)^k$ and the fact that $|\underline{\lambda} \cdot \mathbf{x}| \leq c_1 D$ for each $\underline{\lambda} \in \mathbb{N}^d$ with $|\underline{\lambda}| \leq D$. This gives

$$\sum_{k=K}^{\infty} \sum_{|\underline{\lambda}| \leq D} \frac{|\underline{\lambda} \cdot \mathbf{x}|^k r^k}{k!} \leq n \sum_{k=K}^{\infty} \left(\frac{c_1 e D r}{k} \right)^k.$$

Again, since $\nu > \alpha + \rho$, we have $c_1 e D r \leq K/e$ if N is large enough and so

$$\sum_{k=K}^{\infty} \left(\frac{c_1 e D r}{k} \right)^k \leq \sum_{k=K}^{\infty} e^{-k} \leq 2\exp(-K).$$

Combining the last two inequalities and substituting the result into (9), we conclude that

$$|f|_r \leq K \exp(-2V) + 2n \exp(N^\beta - K) \leq \exp(-V)$$

if N is large enough. □

References

[1] G. Diaz, Grands degrés de transcendance pour des familles d'exponentielles, *J. Number Theory* **31** (1989), 1–23.

[2] A. O. Gel'fond, On the algebraic independence of transcendental numbers of certain classes, *Uspehi Matem. Nauk (N.S.)* **4**, no. 5 (33), (1949), 14–48 (Russian).

[3] P. Philippon, Critères pour l'indépendance algébrique, *Pub. Math. IHES*, **64** (1986), 5-52.

[4] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Math., vol. 785, Springer-Verlag, 1980.

[5] C. L. Siegel, *Transcendental numbers*, Princeton U. Press, 1949.

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

[7] M. Waldschmidt, Algebraic independence in algebraic groups. Part II: Large transcendence degrees, in: *Introduction to Algebraic Independence Theory*, Eds: Yu. V. Nesterenko and P. Philippon, Lecture Notes in Math., vol. 1752, Springer, 2001.