Advances in Number Theory

The Proceedings of the Third Conference of the Canadian Number Theory Association
August 18–24, 1991
The Queen's University at Kingston

Edited by

FERNANDO Q. GOUVÊA
Department of Mathematics and Computer Science, Colby College
and
NORIKO YUI
Department of Mathematics and Statistics, Queen's University

in consultation with
A. Granville, R. Gupta, E. Kani, H. Kisilevsky,
R. Mollin, and C. Stewart

CLARENDON PRESS · OXFORD
1993

Transcendental Numbers and Functions of Several Variables

Michel Waldschmidt
Université P. et M. Curie (Paris VI)

SUMMARY. We start by two density problems: one was raised by Sansuc and deals with algebraic number fields, the other is a question of Mazur and deals with abelian varieties. While the first has just been completely solved by D.Roy, only partial answers have been obtained so far for the second. In both cases the main tool is the theorem of the algebraic subgroup.

We show that this theorem enables one to recover Baker's result on linear combinations of logarithms of algebraic numbers in at least four different ways. Another consequence, once more due to R. Roy, concerns matrices whose entries are linear combinations of logarithms of algebraic numbers.

The proof of the algebraic subgroup theorem is briefly explained, by means of an interpolation determinant, following an idea of M. Laurent. Finally we show how the transposition of the interpolation matrix is connected with a duality in transcendence proofs.

1. Two density problems

[1] *A question of Sansuc*

Let k be a number field of degree $[k:\mathbb{Q}] = n = r_1 + 2r_2$, where, as usual, r_1 (resp. r_2) denotes the number of real (resp. the number of pairs of complex conjugate) embeddings of k into $\mathbb{R}$ (resp. into $\mathbb{C}$). The tensor product $(\mathbb{R}\otimes_{\mathbb{Q}} k)^\times$ is nothing else than $\mathbb{R}^{\times r_1} \times \mathbb{C}^{\times r_2}$. Since the topological group $\mathbb{R}^\times$ (resp. $\mathbb{C}^\times$) is isomorphic to $\mathbb{R}_+^\times \times \mathbb{Z}/2\mathbb{Z}$ (resp $\mathbb{R}_+^\times \times \mathbb{R}/\mathbb{Z}$), and since $\mathbb{R}_+^\times$ is isomorphic to $\mathbb{R}$, the canonical embedding of $k^\times$ into $(\mathbb{R}\otimes_{\mathbb{Q}} k)^\times$ gives rise to an injective homomorphism

$$k^\times \longrightarrow \mathbb{R}^{r_1+r_2} \times (\mathbb{R}/\mathbb{Z})^{r_2} \times (\mathbb{Z}/2\mathbb{Z})^{r_1}.$$

The image of $k^\times$ is dense; Colliot-Thélène and Sansuc asked whether there exists a finitely generated subgroup of $k^\times$ whose image is dense; then Sansuc [Sa] asked for the smaller rank of such a finitely generated subgroup. The complete answer to this question has just been obtained by D. Roy [R3]:

Theorem 1. *There exists a finitely generated subgroup of* $k^\times$ *of rank* $r_1 + r_2 + 1$ *which is dense in* $(\mathbb{R}\otimes_{\mathbb{Q}} k)^\times$.

The proof splits in two parts. The first one is a <u>topological argument</u>: let Y_0 be a discrete subgroup of $\mathbb{R}^n$ and Y a finitely generated subgroup of $\mathbb{R}^n$ containing Y_0. If no subgroup of Y of rank $n+1$ containing Y_0 is dense in $\mathbb{R}^n$, then there exists a finitely generated subgroup of Y of rank $\geq \mathrm{rk}Y - n + 1$ which contains Y_0 and is dense in $\mathbb{R}^n$. In the special case we are dealing with, we take for Y_0 the kernel of the exponential map

$$\exp : \mathbb{R} \otimes_{\mathbb{Q}} k \longrightarrow (\mathbb{R} \otimes_{\mathbb{Q}} k)^{\times}.$$

We refer to Roy's paper [R3] for more detailed information on the topological argument. We shall be mainly concerned here with the second part of the proof, which is a <u>transcendence argument</u>: let $\alpha_1, \ldots, \alpha_\ell$ in $k^\times$ be such that the ℓn numbers $\sigma_i\alpha_j$, $(1 \leq i \leq n,\ 1 \leq j \leq \ell)$ are multiplicatively independent. Choose $y_1, \ldots, y_\ell$ in $\mathbb{R} \otimes_{\mathbb{Q}} k$ such that

$$\exp y_j = (\sigma_1\alpha_j, \ldots, \sigma_n\alpha_j), \qquad 1 \leq j \leq \ell.$$

If $\ell \geq n^2 - n + 2$, then any subgroup of $Y = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$ of rank $\geq n^2 - n + 2$ is dense $\mathbb{R} \otimes_{\mathbb{Q}} k$. In particular if $\ell \geq n^2 + 1$, then any subgroup of Y of rank $\geq \mathrm{rk}Y - n + 1$ is dense $\mathbb{R} \otimes_{\mathbb{Q}} k$.

We discuss more thoroughly this statement below.

[2] *A question of Mazur*

The following question is a special case of a much more general situation considered by B. Mazur [M]. Let A be a simple abelian variety over $\mathbb{Q}$ of dimension $d \geq 1$ with Mordell-Weil group $A(\mathbb{Q})$ of positive rank. Does the connected component of 0 in the topological closure of $A(\mathbb{Q})$ coincide with the connected component $A(\mathbb{R})_0$ of 0 in $A(\mathbb{R})$?

We can provide a positive answer if we assume that the rank of $A(\mathbb{Q})$ is sufficiently large:

Theorem 2. *Assume* $\mathrm{rk}_{\mathbb{Z}}A(\mathbb{Q}) \geq d^2 - d + 1$. *Then* $A(\mathbb{Q}) \cap A(\mathbb{R})_0$ *is dense in* $A(\mathbb{R})_0$.

Remark. Using the above mentioned topological argument of D.Roy, one can also show that if $\mathrm{rk}_{\mathbb{Z}}A(\mathbb{Q}) \geq d^2$, then there is a $u \in A(\mathbb{Q})$ such that $\mathbb{Z}u$ is dense in $A(\mathbb{R})_0$.

In both examples, we are dealing with a finitely generated subgroup of a real vector space. The following easy lemma will reduce the topological problem to an algebraic question: how many independent points of this subgroup can lie in a given hyperplane?

Lemma 3. *Let $Y = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$ be a finitely generated subgroup of a $\mathbb{R}$-vector space E of dimension d. Then Y is dense in E if and only if for each hyperplane V of E,*

$$\mathrm{rk}_{\mathbb{Z}} Y/Y \cap V \geq 2.$$

Writing V as the kernel of a linear form, we can state this condition as follows: *for each non-zero $\varphi \in \mathrm{Hom}_{\mathbb{R}}(E, \mathbb{R})$, one has $\varphi(Y) \not\subset \mathbb{Z}$.*

Let us come back to our two special cases.

[1] *First example* (Sansuc).

We denote by $\bar{\mathbb{Q}}$ the field of algebraic numbers (algebraic closure of $\mathbb{Q}$ into $\mathbb{C}$), and by $\mathbb{L}$ the $\mathbb{Q}$–vector space of logarithms of algebraic numbers:

$$\mathbb{L} = \{\log \alpha; \alpha \in \bar{\mathbb{Q}}^\times\} = \{z \in \mathbb{C}; e^z \in \bar{\mathbb{Q}}^\times\}.$$

Michel Emsalem first noticed that if V is an hyperplane of $\mathbb{C}^d$ with $V \cap \mathbb{Q}^d \neq \{0\}$, then

$$\dim_{\mathbb{Q}} V \cap \mathbb{L}^d = \infty;$$

indeed, assume $0 \neq (b_1, \ldots, b_d) \in V \cap \mathbb{Q}^d$; then for all $\log \alpha \in \mathbb{L}$,

$$(b_1 \log \alpha, \ldots, b_d \log \alpha) \in V \cap \mathbb{L}^d,$$

which proves the claim. Emsalem [E] also proved the converse: *if V is an hyperplane of $\mathbb{C}^d$ with $V \cap \mathbb{Q}^d = \{0\}$, then*

$$\dim_{\mathbb{Q}} V \cap \mathbb{L}^d < \infty.$$

Using lemma 3, we now show that the first part of the proof of theorem 1 is a consequence of the following:

Transcendence result: if $V \cap \mathbb{Q}^d = \{0\}$, then

$$\dim_{\mathbb{Q}} V \cap \mathbb{L}^d \leq d(d-1).$$

This transcendence result, due to M. Emsalem [E], will be deduced later from the theorem of the algebraic subgroup.

Consequence: let Y' be a subgroup of $\mathbb{L}^d$ of rank $\ell' \geq d^2 - d + 2$; for each hyperplane V with $V \cap \mathbb{Q}^d = \{0\}$ we obtain the bound $\mathrm{rk}_{\mathbb{Z}}(Y' \cap V) \leq d(d-1)$, hence $\mathrm{rk}_{\mathbb{Z}}(Y'/Y' \cap V) \geq 2$. We need to consider also the hyperplanes V with $V \cap \mathbb{Q}^d \neq \{0\}$. Assume Y' is contained in a finitely generated subgroup Y of $\mathbb{L}^d$, and Y is generated by ℓ elements of $\mathbb{L}^d$ such that the ℓd components of the generators are linearly independent over $\mathbb{Q}$. Let S be the subspace of $\mathbb{C}^d$ generated by $V \cap \mathbb{Q}^d$; this is the maximal subspace of $\mathbb{C}^d$ which is rational over $\mathbb{Q}$ and contained in V. We write S as intersection of

δ hyperplanes $\varphi_1 = 0, \ldots, \varphi_\delta = 0$, where $\varphi_1, \ldots, \varphi_\delta$ are linear forms on $\mathbb{C}^d$ with rational coefficients. Hence $\varphi = (\varphi_1, \ldots, \varphi_\delta)$ is a surjective linear map from $\mathbb{C}^d$ onto $\mathbb{C}^\delta$ with kernel S, and $V' = \varphi(V)$ satisfies $V' \cap \mathbb{Q}^\delta = 0$. On the other hand our assumption on Y is more than enough to ensure $Y \cap S = 0$, hence $Y'' = \varphi(Y')$ is again of rank ℓ'. We apply the transcendence result to $Y'' \subset \mathbb{L}^d$ and deduce $\mathrm{rk}(Y'' \cap V') \leq \delta(\delta-1)$. Therefore $\mathrm{rk}(Y' \cap V) \leq d(d-1)$ and $\mathrm{rk}(Y'/Y' \cap V) \geq 2$ for all hyperplanes V of $\mathbb{C}^d$.

2 *Second example* (Mazur).

Let A be an abelian variety which is defined over $\bar{\mathbb{Q}}$. We denote by T_A the tangent space of A at the origin, and by $\exp : T_A(\mathbb{C}) \to A(\mathbb{C})$ the exponential map of the Lie group $A(\mathbb{C})$. The complex vector space $T_A(\mathbb{C})$ is of dimension $d = \dim A$ and its kernel (periods of the exponential map) is a lattice in $T_A(\mathbb{C})$ (discrete subgroup of rank $2d$).

We consider the $\mathbb{Q}$-vector space of logarithms of algebraic points on A:

$$\Lambda = \exp_A^{-1} A(\bar{\mathbb{Q}}) \subset T_A(\mathbb{C}).$$

We now show that theorem 2 is a consequence of the following statement, which we deduce below from the theorem of the algebraic subgroup:
Transcendence result: if V is a hyperplane of $T_A(\mathbb{C})$ containing $d-1$ independent elements of $\ker \exp_A$, then $\dim_{\mathbb{Q}} V \cap \Lambda \leq d^2 - 1$.

Consequence: assume A is defined over $\mathbb{Q}$; then $T_A(\mathbb{R})$ contains d periods $\omega_1, \ldots, \omega_d$, which are linearly independent over $\mathbb{R}$. Consider m points in $A(\bar{\mathbb{Q}})$ which are linearly independent over $\mathbb{Z}$; we can write these points $\exp_A(u_j) \in A(\bar{\mathbb{Q}})$, $(1 \leq j \leq m)$, and the subgroup

$$Y = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_d + \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subset T_A(\mathbb{R}) \simeq \mathbb{R}^d$$

is contained in Λ, of rank $\mathrm{rk}_{\mathbb{Z}} Y = \ell = m + d$. If $m \geq d^2 - d + 1$, then $\ell \geq d^2 + 1$, and we conclude

$$\mathrm{rk}_{\mathbb{Z}} Y / Y \cap V \geq d^2 + 1 - (d^2 - 1) = 2.$$

2. Theorem of the algebraic subgroup

Let G be an algebraic group defined over $\bar{\mathbb{Q}}$. We denote by Λ the $\mathbb{Q}$-vector space of the logarithms of algebraic points on G:

$$\Lambda = \exp_G^{-1}\bigl(G(\bar{\mathbb{Q}})\bigr).$$

Further, let V be a complex subspace of $T_G(\mathbb{C})$. We consider the intersection $V \cap \Lambda$, which is a $\mathbb{Q}$-vector space, and we denote by ℓ its dimension. A necessary condition for ℓ to be finite is that V does not contain any non-zero tangent subspace of an algebraic subgroup H of G, defined over $\bar{\mathbb{Q}}$:

$$V \not\supset T_H(\mathbb{C}) \neq \{0\}.$$

Examples: firstly, let $G = \mathbb{G}_m^d$, where $\mathbb{G}_m$ is the multiplicative group; in this case $\Lambda = \mathbb{L}^d$, and the above condition reads $V \cap \mathbb{Q}^d = \{0\}$. Secondly, let $G = A$ be a simple abelian variety; then the condition is just $V \neq T_A(\mathbb{C})$.

Theorem 4. *If V is a hyperplane in $T_G(\mathbb{C})$ which does not contain any non-zero subspace of the form $T_H(\mathbb{C})$, (H algebraic subgroup of G defined over $\bar{\mathbb{Q}}$), then $\ell < \infty$.*

We now want to give an explicit upper bound for ℓ, assuming that it is finite. A first estimate, which is valid in the general case, is $\ell \leq 2d(d-1)$. This estimate is sufficient for theorem 1; however our *transcendence argument* related to Sansuc's problem above claimed a stronger upper bound. Indeed, when G is a linear algebraic group then one can sharpen this estimate and get $\ell \leq d(d-1)$.

One can produce a bound which is valid in the general case, and includes the refinement in the linear case: we write G as a product $G = G_0 \times G_1 \times G_2$, with $G_0 = \mathbb{G}_a^{d_0}$, $G_1 = \mathbb{G}_m^{d_1}$, $\dim G_2 = d_2$, and $d = d_0 + d_1 + d_2$. This is no loss of generality: we can choose for instance $d_0 = d_1 = 0$, $d_2 = d$. With this notation the following bound for ℓ holds: $\ell \leq (d_1 + 2d_2)(d-1)$.

This estimate is not still sharp enough for theorem 2. In order to have a more precise bound we introduce a further notation: we take into account the number κ of independent periods of $\exp_G$ which sit in V:

$$\kappa = \mathrm{rk}_{\mathbb{Z}}\big(V \cap \ker \exp_G\big).$$

Then $\ell \leq (d_1 + 2d_2 - \kappa)(d-1)$.

For Mazur's problem we choose $d_0 = d_1 = 0$, $d_2 = d$, $\kappa = d-1$, and we conclude $\ell \leq d^2 - 1$.

A further refinement will be needed below: we count how many independent points of $T_G(\mathbb{C})$ which are rational over $\bar{\mathbb{Q}}$ lie inside V (recall that T_G has a natural $\bar{\mathbb{Q}}$–structure, since it is the tangent space of the algebraic group G which is defined over $\bar{\mathbb{Q}}$).

Theorem 4 (continued). *If $V \supset W$ with W rational over $\bar{\mathbb{Q}}$, then*

$$\ell \leq (d_1 + 2d_2 - \kappa)\dim_{\mathbb{C}}(V/W).$$

There is a more general result ([W1] theorem 4.1) but the statement is slightly more complicated.

This theorem of the algebraic subgroup includes essentially all known transcendence results on analytic subgroups of commutative group varieties (apart from results of algebraic independence). The first statements of this form dealing with several parameter subgroups go back to Schneider's works in the first half of this century. In particular his paper [S], where he proves the transcendence of values of the Beta function at rational points, introduces for the first time functions of several complex variables in transcendental number theory. The subject was taken up again by Lang in the 60's [L]; like in Schneider's work, the analytic argument is an interpolation formula for a cartesian product in $\mathbb{C}^n$. The main transcendence result (*Schneider–Lang criterion*) concerns the values on a cartesian product of analytic functions satisfying differential equations; one main point is that the cartesian product does not involve the same system of coordinates than the differential equations, and this is why the result does not reduce to its one dimensional analog; it is useful for applications to so-called *normalized* n-parameter subgroups of algebraic groups [L]. A deeper Schwarz lemma in higher dimension, using Lelong's measure for the area of the analytic hypersurface of zeros of an analytic function, was proved by Bombieri and Lang in [B-L], and they used it to study non-normalized n-parameter subgroups of algebraic groups; but the result they obtain involves very strong repartition results which seem out of reach of the present theory of diophantine approximations. Then Bombieri [B] introduced in the theory the L^2-estimates of Hörmander and replaced the cartesian product by a more natural condition (conjectured by Nagata) that the considered points do not lie in an algebraic hypersurface; but it turns out that these tools do not yield further transcendence results in connection with algebraic groups.

Nowadays, these ingredients from the theory of functions in several variables are no longer useful: the analytic argument is reduced to the very easy Schwarz lemma for functions of a single variable [W2]; on the other hand a very important role is played by a geometrical tool, the zero estimate [P].

In the case $V = W$, the conclusion of theorem 4 is $\ell = 0$. This is a result of Wüstholz [Wü] which rests on Baker's method. The proof of this special case does not involve functions of several variables, since it is sufficient to work with one point and its multiples, which all lie on a complex line in $T_G(\mathbb{C})$.

3. Linear combinations of logarithms of algebraic numbers

In this section we deduce from the algebraic subgroup theorem the following well known result of Baker:

Theorem 5. *Let* $\log\alpha_1, \dots, \log\alpha_n$ *be elements in* $\mathbb{L}$, *not all of which are zero, and let* $\beta_1, \dots, \beta_n$ *be algebraic numbers, not all zero. If we have* $\beta_1 \log\alpha_1 + \cdots + \beta_n \log\alpha_n = 0$, *then* $\beta_1, \dots, \beta_n$ *are* $\mathbb{Q}$*-linearly dependent, and* $\log\alpha_1, \dots, \log\alpha_n$ *are* $\mathbb{Q}$*-linearly dependent.*

We give four sketches of proof of theorem 5 as a consequence of theorem 4 with $d_2 = \kappa = 0$. We start with a non-trivial relation of minimal length n

between logarithms of algebraic numbers with algebraic coefficients; since n is minimal, it is plainly sufficient to prove either that the β's are $\mathbb{Q}$-linearly dependent, or that the $\log\alpha$'s are $\mathbb{Q}$-linearly dependent.

[1] *Baker's method*

Let us choose $d_0 = 0$ and $d = d_1 = n$; in this case $\Lambda = \mathbb{L}^n$. We take for V the hyperplane of equation $\beta_1 z_1 + \cdots + \beta_n z_n = 0$ in $\mathbb{C}^n$, and we choose $W = V$. In this case

$$V \cap \Lambda \ni (\log\alpha_1, \ldots, \log\alpha_n) \neq 0,$$

which shows that $\ell > 0$. The theorem of the algebraic subgroup implies $V \cap \mathbb{Q}^n \neq \{0\}$ and therefore $\beta_1, \ldots, \beta_n$ are $\mathbb{Q}$-linearly dependent.

[2] *Hirata's method*

The choice here is $d_0 = 1$, $d_1 = n$, $d = n+1$, hence $\Lambda = \bar{\mathbb{Q}} \times \mathbb{L}^n$. Let $V = W$ be the hyperplane of equation $z_0 = \beta_1 z_1 + \cdots + \beta_n z_n$ in $\mathbb{C}^{n+1}$. Since

$$V \cap \Lambda \ni (0, \log\alpha_1, \ldots, \log\alpha_n) \neq 0,$$

we have $\ell > 0$, and theorem 4 implies $V \supset T_H \neq \{0\}$, which means that $\beta_1, \ldots, \beta_n$ are $\mathbb{Q}$-linearly dependent.

[3] *Dual of Baker's method*

We now choose $d_0 = n-1$, $d_1 = 1$, $d = n$, so that $\Lambda = \bar{\mathbb{Q}}^{n-1} \times \mathbb{L}$. Further let $W = \{0\}$, and let V be the hyperplane kernel of the linear form $z_1 \log\alpha_1 + \cdots + z_{n-1}\log\alpha_{n-1} + z_n$. For $(h_1, \ldots, h_n) \in \mathbb{Z}^n$ we have

$$V \cap \Lambda \ni \big(h_1, \ldots, h_{n-1}, h_1 \log\alpha_1 + \cdots + h_{n-1}\log\alpha_{n-1}\big)$$

and

$$V \cap \Lambda \ni \left(h_n \frac{\beta_1}{\beta_n}, \ldots, h_n \frac{\beta_{n-1}}{\beta_n}, h_n \log\alpha_n\right),$$

Therefore $\ell \geq n$, hence $V \supset T_H \neq \{0\}$. One therefore deduces that $\log\alpha_1, \ldots, \log\alpha_{n-1}$ are $\bar{\mathbb{Q}}$-linearly dependent, which contradicts our choice of n minimal.

[4] *Dual of Hirata's method*

The duality that we shall describe at the end of this lecture suggests to choose $d_0 = n$, $d_1 = 1$, $d = n+1$, hence $\Lambda = \bar{\mathbb{Q}}^n \times \mathbb{L}$, and then $W =$

$\mathbb{C}(\beta_1,\ldots,\beta_n,0)$, while V is once more an hyperplane: $z_{n+1} = z_1\log\alpha_1 + \cdots + z_n\log\alpha_n$. For $(h_1,\ldots,h_n)\in\mathbb{Z}^n$ we have

$$V\cap\Lambda \ni (h_1,\ldots,h_n,h_1\log\alpha_1+\cdots+h_n\log\alpha_n);$$

therefore $\ell \geq n$, and $V \supset T_H \neq \{0\}$. But here we already know that V contains a non-zero subspace of this form, namely W which is the tangent space of the additive group, image of $\mathbb{G}_a \longrightarrow \mathbb{G}_a^n \times \mathbb{G}_m$ by

$$z \longmapsto (\beta_1 z,\ldots,\beta_m z, 1).$$

Instead of this we work with the quotient V/W; we are back to a situation similar to that in method 3, except that we do not loose the symmetry between $\log\alpha_1,\ldots,\log\alpha_n$, and also the choice of the parameters is substantially different (see [W3]).

It is possible to develop the four methods in order to provide explicit estimates. This is well known for the first method (Baker's theory). The second method has been introduced by N. Hirata–Kohno in her study of lower bounds for linear forms on algebraic commutative groups [H]. The third and fourth method have been used in [W3] and provide sharp estimates; here is an example which has been worked out using method 3:

Theorem 6. *Let $a_1,\ldots,a_n$ be rational integers, $a_i\geq 2$, and let $b_1,\ldots,b_n$ be rational integers with $a_1^{b_1}\cdots a_n^{b_n}\neq 1$. Define $B=\max\{2,|b_1|,\ldots,|b_n|\}$; then*

$$\left|a_1^{b_1}\cdots a_n^{b_n}-1\right| \geq \exp\{-2^{4n+16}n^{3n+5}\log B\log a_1\cdots\log a_n\}.$$

In methods 1 and 2, the points we consider in $V\cap\Lambda$ all lie on a complex line (subspace of dimension 1); this fact has been an essential feature of Baker's method up to recently (see for instance [Wü], and also [H]): it enables one to use interpolation techniques, and to work out the proof without introducing functions of several variables. The situation is quite different for the two dual methods, where the points span a vector space of higher dimension (as soon as $n\geq 3$ for method 3, and also for $n=2$ in method 4). In this case there is so far no available extrapolation argument, and because of this the method is more primitive. The main fact which enables us to derive sharp bounds is that there is a single factor $\mathbb{G}_m$ (i.e. only one exponential function); cf [W2] and [W3].

4. Matrices whose entries are linear combinations of logarithms

One motivation for the results in this section is Leopoldt's conjecture on the p-adic rank of units of an algebraic number field. When one considers an algebraic number field which is Galois over $\mathbb{Q}$, the action of the Galois group gives rise to a block decomposition of the the p-adic regulator into square matrices whose entries are linear combinations with algebraic coefficients of p-adic logarithms of algebraic numbers. The problem is to give a lower bound for the rank of such matrices.

We consider here only the complex case, but the results can be extended also to non-archimedean fields.

Let M be a $d \times \ell$ matrix whose entries are linear combinations of (complex) logarithms of algebraic numbers. The coefficients of M belong to a $\bar{\mathbb{Q}}$-vector space generated by $\mathbb{Q}$-linearly independent elements $\log \alpha_1, \ldots, \log \alpha_s$ of L ; hence one can write

$$M = \left(\beta_{0ij} + \sum_{s=1}^{S} \beta_{sij} \log \alpha_s \right)_{\substack{1 \le i \le d, \\ 1 \le j \le \ell}} = B_0 + \sum_{s=1}^{S} B_s \log \alpha_s$$

with $\log \alpha_s$ linearly independent over $\mathbb{Q}$ (or over $\bar{\mathbb{Q}}$) and $B_0, \ldots, B_S$ matrices with algebraic entries.

Following D.Roy [R1], one defines the *structural rank* $r_{\mathrm{conj}}(M)$ of M as the rank of the matrix

$$B_0 + \sum_{s=1}^{S} B_s X_s$$

in $\bar{\mathbb{Q}}(X_1, \ldots, X_S)$. From the standard conjecture stating that $\mathbb{Q}$-linearly independent elements of $\mathbb{L}$ are algebraically independent over $\mathbb{Q}$ (hence over $\bar{\mathbb{Q}}$), one immediately deduces:

Conjecture 7.

$$\mathrm{rk}(M) = r_{\mathrm{conj}}(M).$$

It happens often in this subject that one is able to prove half of what one expects; in the present case, D.Roy proved [R1]:

Theorem 8.

$$\mathrm{rk}(M) \geq \frac{1}{2} r_{\mathrm{conj}}(M).$$

Here is a connection with the situation we considered in theorem 4: if $\mathrm{rk}(M) < d$, then the ℓ columns vectors

$$u_j = \left(\beta_{0ij} + \sum_{s=1}^{S} \beta_{sij} \log \alpha_s \right)_{1 \le i \le d}, \qquad (1 \le j \le \ell)$$

belong to a hyperplane of $\mathbb{C}^d$; denote by $\mathcal{L}$ the $\bar{\mathbb{Q}}$-vector space spanned by 1 and $\mathbb{L}$ in $\mathbb{C}$:

$$\mathcal{L} = \{\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \, ; \, \beta_i \in \bar{\mathbb{Q}}, \, \log \alpha_i \in \mathbb{L}\}.$$

Let V be a complex vector subspace of $\mathbb{C}^d$; if $V \cap \bar{\mathbb{Q}}^d \ni (\beta_1, \ldots, \beta_d) \neq 0$, then

$$(\beta_1 \log \alpha, \ldots, \beta_d \log \alpha) \in V \cap \mathcal{L}^d$$

for all $\log \alpha \in \mathbb{L}$; hence $\dim_{\bar{\mathbb{Q}}} V \cap \mathcal{L}^d = \infty$. As shown by D. Roy [R1], the converse is true: if $\dim_{\bar{\mathbb{Q}}} V \cap \mathcal{L}^d = \infty$, then $V \cap \bar{\mathbb{Q}}^d \ni (\beta_1, \ldots, \beta_d) \neq 0$. More precisely:

Theorem 9. *If $V \cap \bar{\mathbb{Q}}^d = \{0\}$, then*

$$\dim_{\bar{\mathbb{Q}}} V \cap \mathcal{L}^d \leq d(d-1).$$

This result is in fact a consequence of theorem 4 (this is not obvious). In a joint work with Damien Roy [R-W], we develop the idea of [R1] and study the following generalization of theorem 9: let again G be an algebraic group defined over $\bar{\mathbb{Q}}$; we consider once more the $\mathbb{Q}$-vector space $\Lambda = \exp_G^{-1} G(\bar{\mathbb{Q}})$ in $T_G(\mathbb{C})$. Now let K be a number field; define Λ_K as the K-vector space spanned by Λ in $T_G(\mathbb{C})$:

$$\Lambda_K = \{\beta_1 u_1 + \cdots + \beta_n u_n \,;\, n \geq 0,\, \beta_i \in K,\, \exp_G u_i \in G(\bar{\mathbb{Q}})\}.$$

For $m \geq 1$ and $\beta = (\beta_1, \ldots, \beta_m) \in K^m$, consider the map

$$\begin{array}{cccc} \varphi_\beta: & T_{G^m} & \longrightarrow & T_G \\ & (z_1, \ldots, z_m) & \longmapsto & z_1\beta_1 + \cdots + z_m\beta_m \end{array}$$

If G' is an algebraic subgroup of G^m defined over $\bar{\mathbb{Q}}$ of positive dimension such that $\varphi_\beta(T_{G'}) \subset V$, then for each $u \in T_{G'}(\mathbb{C})$ with $\exp_{G'} u \in G'(\bar{\mathbb{Q}})$, we have $\varphi_\beta(u) \in V \cap \Lambda_K$. Therefore $\dim_K V \cap \Lambda_K = \infty$. Here is the converse:

Theorem 10. *If V does not contain any non-zero subspace of the form $\varphi_\beta(T_{G'})$, then*

$$\dim_K V \cap \Lambda_K \leq (d_1 + 2d_2) \dim_{\mathbb{C}}(V/W).$$

5. Interpolation determinants

This last section is devoted to a sketch of proof of the algebraic subgroup theorem. The original proof [W1] used the classical transcendence method of Gel'fond-Schneider, with a construction of an auxiliary function performed thanks to the Dirichlet box principle (lemma of Thue-Siegel). Here, we follow an idea of Michel Laurent [La] and consider an interpolation determinant:

$$\Delta = \det\big(\varphi_\lambda(\zeta_\mu)\big)_{1 \leq \lambda, \mu \leq N}.$$

The main analytic argument is the following:

Lemma 11. *Let $\varphi_1, \ldots, \varphi_N$ be analytic functions in a polydisk $\{z \in \mathbb{C}^n \; ; \; |z| \leq R\}$ in $\mathbb{C}^n$, and let $\zeta_1, \ldots, \zeta_N$ in $\mathbb{C}^n$ satisfy $|\zeta_\mu| \leq r < R$. Then*

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-T} N! \prod_{\lambda=1}^{N} |\varphi_\lambda|_R$$

with

$$T \geq \frac{n}{6e} N^{(n+1)/n} \qquad \text{for} \quad N \geq 2^n e^{n+1}.$$

This lemma is fundamental for the proof below; its proof just uses the classical Schwarz lemma for functions of one complex variable with a high order multiplicity of zero at the origin.

Here is a sketch of proof of the algebraic subgroup theorem using lemma 11. We take linearly independent points $y_1, \ldots, y_\ell$ in $V \cap \Lambda$; the interpolation points will be indexed by $h = (h_1, \ldots, h_\ell) \in \mathbb{Z}^\ell$ with $0 \leq h_j < H$, $(1 \leq j \leq \ell)$:

$$\xi_h = h_1 y_1 + \cdots + h_\ell y_\ell.$$

We consider the functions $\varphi_\lambda = f_0^{\lambda_0} \cdots f_M^{\lambda_M} / f_0^L$, where $(\lambda_0, \ldots, \lambda_M) \in \mathbb{Z}^{M+1}$, $\lambda_0 + \cdots + \lambda_M = L$, and $(f_0, \ldots, f_M)$ are entire functions which give a representation the exponential map $\exp_G : T_G(\mathbb{C}) \longrightarrow G(\mathbb{C})$ composed with an embedding of $G(\mathbb{C})$ into a projective space $\mathbb{P}_M(\mathbb{C})$. We restrict the values of $\lambda = (\lambda_0, \ldots, \lambda_M)$ so that the φ_λ are linearly independent. Further, the vector subspace W of $T_G(\mathbb{C})$ in theorem 4 provides derivations which we write D_W^τ, $(\tau \in \mathbb{N}^t$ with $t = \dim_{\mathbb{C}} W)$ which have the crucial property:

$$D_W^\tau \varphi_\lambda(\xi_h) \in \bar{\mathbb{Q}}, \quad \text{for all} \quad \tau \in \mathbb{N}^t.$$

We shall use this information only for $||\tau|| \leq T$, where T is a new parameter.

The main steps of the proof are as follows:

1. One starts by choosing the parameters L, T and H. In practice, one first writes the conditions that these parameters have to satisfy in such a way that the four steps below work, then one optimizes the choice of these parameters, and finally one writes down the proof starting with this choice. The final result depends heavily on these estimates, and there is no other justification than these computations to explain the explicit upper bound we finally obtain.

2. Here comes the geometric part of the proof, with the zero estimate of Philippon; it enables one to choose a subset $\mathcal{H}$ of $\{h = (h_1, \ldots, h_\ell) \in \mathbb{Z}^\ell \; ; \; 0 \leq h_j < H, \; (1 \leq j \leq \ell)\}$, such that the determinant

$$\Delta = \det\left(D_W^\tau \varphi_\lambda(\xi_h)\right)_{\binom{\lambda, \tau}{h \in \mathcal{H}}}$$

does not vanish.

3. The analytic part of the proof is provided by lemma 11 of M.Laurent (the fact that the φ_λ are meromorphic rather than analytic is not a serious difficulty); one deduces an upper bound for $|\Delta|$, say $|\Delta| \leq \epsilon_1$.

4. The arithmetic argument is nothing else than the classical Liouville estimate; since Δ is a non-zero algebraic number, it cannot be too small: $|\Delta| \geq \epsilon_2$.

5. Now comes the conclusion: $\epsilon_2 \leq \epsilon_1$. There is still some work to do to get the desired statement; in fact the zero estimate yields a non-zero Δ provided that not too many points of $\mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$ lie in the tangent space of a proper algebraic algebraic subgroup of G. But we shall not give more details here (see [W1] for a complete proof).

6. Duality

We end this lecture by a discussion of a duality in transcendence proofs. We consider the following easy identity:

$$(d/dz)^\tau \left(z^\sigma e^{xz}\right)_{z=y} = (d/dz)^\sigma \left(z^\tau e^{yz}\right)_{z=x}$$

where x, y, z are complex numbers while σ and τ are non-negative integers.

There is a generalization of this identity to several variables [W2]: let n, t, s be positive integers, $x, y, z, w_1, \ldots, w_t, u_1, \ldots, u_s \in \mathbb{C}^n$, and $\sigma \in \mathbb{N}^s$, $\tau \in \mathbb{N}^t$; define ζz as the standard scalar product in $\mathbb{C}^n$, namely $\zeta z = \zeta_1 z_1 + \cdots + \zeta_n z_n$, and similarly $D_\zeta = \zeta_1(\partial/\partial z_1) + \cdots + \zeta_n(\partial/\partial z_n)$; then

$$D_{w_1}^{\tau_1} \cdots D_{w_t}^{\tau_t} \left((u_1 z)^{\sigma_1} \cdots (u_s z)^{\sigma_s} e^{xz}\right)_{z=y} =$$

$$= D_{u_1}^{\sigma_1} \cdots D_{u_s}^{\sigma_s} \left((w_1 z)^{\tau_1} \cdots (w_t z)^{\tau_t} e^{yz}\right)_{z=x}$$

This relation occurs in the proofs of theorem 5 as follows: assume we have a non-trivial linear relation $\log \alpha_n = \beta_1 \log \alpha_1 + \cdots + \beta_{n-1} \log \alpha_{n-1}$ and define, for $h = (h_1, \ldots, h_n) \in \mathbb{Z}^n$, $\tau = (\tau_1, \ldots, \tau_{n-1}) \in \mathbb{Z}^{n-1}$ and $\lambda \in \mathbb{Z}$:

$$\gamma_{h;\tau,\lambda} = \prod_{i=1}^{n-1} (h_i + h_n \beta_i)^{\tau_i} \prod_{j=1}^{n} \alpha_j^{\lambda h_j};$$

these numbers $\gamma_{h;\tau,\lambda}$ are interpolation values of analytic functions in two different ways: on one hand

$$\gamma_{h;\tau,\lambda} = \left(\frac{\partial}{\partial z_1}\right)^{\tau_1} \cdots \left(\frac{\partial}{\partial z_{n-1}}\right)^{\tau_{n-1}} \psi_h(\lambda \log \alpha_1, \ldots, \lambda \log \alpha_{n-1}),$$

with

$$\psi_h(z_1, \ldots, z_{n-1}) = e^{(h_1 + h_n \beta_1) z_1} \cdots e^{(h_{n-1} + h_n \beta_{n-1}) z_{n-1}};$$

on the other

$$\gamma_{h;\tau,\lambda} = \varphi_{\tau,\lambda}(h_1 + h_n\beta_1, \ldots, h_{n-1} + h_n\beta_{n-1})$$

where

$$\varphi_{\tau,\lambda}(z_1, \ldots, z_{n-1}) = z_1^{\tau_1} \cdots z_{n-1}^{\tau_{n-1}} \left(\alpha_1^{z_1} \cdots \alpha_{n-1}^{z_{n-1}}\right)^{\lambda}.$$

If one specializes the preceding proof to the special case of theorem 5, depending on whether one express $\gamma_{h;\tau,\lambda}$ in terms of $\varphi_{\tau,\lambda}$ or in terms of ψ_h, one recognizes Baker's method or its dual.. For Hirata's method and its dual, one writes, for $\tau \in \mathbb{N}^n$, $h \in \mathbb{N}^{n+1}$ and $\lambda \in \mathbb{Z}$

$$\left(\frac{\partial}{\partial z_1}\right)^{\tau_1} \cdots \left(\frac{\partial}{\partial z_n}\right)^{\tau_n} \tilde{\psi}_h(\lambda \log \alpha_1, \ldots, \lambda \log \alpha_n) = \left(\sum_{i=1}^{n} \beta_i \left(\frac{\partial}{\partial z_i}\right)\right)^{h_0} \tilde{\varphi}_{\tau,\lambda}(h_1, \ldots, h_n),$$

where

$$\tilde{\psi}_h(z_1, \ldots, z_n) = (\beta_1 z_1 + \cdots + \beta_n z_n)^{h_0} e^{h_1 z_1} \cdots e^{h_n z_n}$$

and

$$\tilde{\varphi}_{\tau,\lambda}(z_1, \ldots, z_n) = z_1^{\tau_1} \cdots z_n^{\tau_n} \left(\alpha_1^{z_1} \cdots \alpha_n^{z_n}\right)^{\lambda}$$

References

[B] Bombieri, E. Algebraic values of meromorphic maps. Invent. Math. **10** (1970), 267–287 and **11** (1970), 163–166.

[B-L] Bombieri, E, and Lang, S. Analytic subgroups of group varieties. Invent. Math. **11** (1970), 1–14.

[E] Emsalem, M. Sur les idéaux dont l'image par l'application d' Artin dans une $\mathbb{Z}_p$-extension est triviale. J. reine angew. Math. **382** (1987), 181–198.

[H] N. Hirata. Formes linéaires de logarithmes de points algébriques sur les groupes algébriques. Invent. Math. **104** (1991), 401–433.

[L] Lang, S. *Introduction to transcendental numbers.* Addison Wesley, 1966.

[La] M. Laurent. Hauteur de matrices d'interpolation. in *Approximations Diophantiennes et Nombres Transcendants*, éd. P. Philippon, Proc. Conf. Luminy 1990, W. de Gruyter, à paraître.

[M] B. Mazur. The topology of rational points. Experimental Mathematics **1** (1992), 35–45.

[P] P. Philippon. Lemmes de zéros dans les groupes algébriques commutatifs. Bull. Soc. Math. France **114** (1986), 355–383 et **115** (1987), 397–398.

[R1] D. Roy. Matrices whose coefficients are linear forms in logarithms. J. Number Theory, to appear.

[R2] D. Roy. Transcendance et questions de répartition dans les groupes algébriques. in *Approximations Diophantiennes et Nombres Transcendants*, éd. P. Philippon, Proc. Conf. Luminy 1990, W. de Gruyter, à paraître.

[R3] D. Roy. Simultaneous approximation in number fields .

[R-W] D. Roy et M. Waldschmidt. Autour du théorème du sous-groupe algébrique

[Sa] J-J. Sansuc. Descente et principe de Hasse pour certaines variétés rationnelles. Sém. Théorie des Nombres Delange-Pisot-Poitou, Paris 1980–81, Birkhäuser Verlag, Progress in Math. **22** (1982), 253–271.

[S] Th. Schneider. Zur Theorie des Abelschen Funktionen und Integrale. J. reine angew. Math. **183** (1941), 110–128.

[W1] M. Waldschmidt. On the transcendence methods of Gel'fond and Schneider in several variables. in *New Advances in Transcendence Theory*, ed. A. Baker, Cambridge Univ. Press. 1988, Chap. 24, 375–398.

[W2] M. Waldschmidt. Fonctions auxiliaires et fonctionnelles analytiques. J. Analyse Math., **56** 1991, 231–279.

[W3] M. Waldschmidt. Nouvelles méthodes pour minorer des combinaisons linéaires de logarithmes de nombres algébriques. Sém. Th. Nombres Bordeaux **3** (1991), 129–185; (II), in *Problèmes Diophantiens 1989-1990*, Publ. Univ. P. et M. Curie (Paris VI) **93**, N°8, 36 p.; Minorations de combinaisons linéaires de logarithmes de nombres algébriques. à paraître.

[Wü] G. Wüstholz. Some remarks on a conjecture of Waldschmidt. in *Approximations Diophantiennes et Nombres Transcendants*, éd. D. Bertrand and M. Waldschmidt, Proc. Conf. Luminy 1982, Birkhäuser Verlag, Progress in Math. **31** (1983), 329–336.

Michel Waldschmidt
Université P. et M. Curie (Paris VI)
Problèmes Diophantiens, URA 763 du C.N.R.S.
Institut Henri Poincaré
11, rue P. et M. Curie
F-75231 PARIS Cedex 05
e-mail : miw@frunip62.bitnet