Quadratic relations between logarithms of algebraic numbers

Michel Waldschmidt

May 17, 1996

Abstract. A well known conjecture asserts that **Q**-linearly independent logarithms of algebraic numbers should be algebraically independent. So far it has only been proved that they are linearly independent over the field of algebraic numbers (Baker, 1966). It is not yet known that there exist two logarithms of algebraic numbers which are algebraically independent.

The next step might be to consider quadratic relations between logarithms. However, once more, few results are known. The fact that no non-trivial relation of the form

$$(\log \alpha_1)(\log \alpha_4) = (\log \alpha_2)(\log \alpha_3)$$

can take place is known as the four exponentials conjecture.

We discuss these questions and tell the state of the art on this matter.

The author is thankful to Dr Masami Yoshimoto for his help in the preparation of these notes.

§1. Historical survey

We denote by $\overline{\mathbf{Q}}$ the algebraic closure of the rational number field $\mathbf{Q}$ in the complex field $\mathbf{C}$. By definition, $\overline{\mathbf{Q}}$ is the set of algebraic numbers, viz. the set of complex numbers α for which there exists a nonzero polynomial $P \in \mathbf{Z}[X]$ which vanishes at α.

We also denote by e^z or $\exp(z)$ the usual exponential function, and by

$$\begin{aligned} \mathcal{L} &= \left\{\log\alpha,\ \alpha \in \overline{\mathbf{Q}}^\times\right\} \\ &= \left\{\lambda \in \mathbf{C},\ e^\lambda \in \overline{\mathbf{Q}}^\times\right\} = \exp^{-1}\left(\overline{\mathbf{Q}}^\times\right) \end{aligned}$$

the set of logarithms of algebraic numbers. As $\exp : \mathbf{C} \to \mathbf{C}^\times$ is a group homomorphism and $\overline{\mathbf{Q}}^\times$ a subgroup of $\mathbf{C}$, it follows that $\mathcal{L}$ is an additive subgroup of $\mathbf{C}$. In fact it is not only a $\mathbf{Z}$-submodule, but also a $\mathbf{Q}$-vector subspace of $\mathbf{C}$. This corresponds to the fact that $\overline{\mathbf{Q}}^\times$ is divisible in $\mathbf{C}^\times$, that is for $\alpha \in \overline{\mathbf{Q}}^\times$ and $q \in \mathbf{Z}$, $q > 0$, there exist algebraic numbers $\beta \in \overline{\mathbf{Q}}^\times$ such that $\beta^q = \alpha$. There are several such β's when $q > 1$ (namely q of them, which is the number of q-th roots of unity). Also for a given nonzero complex number α, there are infinitely many λ with $e^\lambda = \alpha$. But when one considers the set of all determinations of logarithms for all algebraic non zero α's, one gets our set $\mathcal{L}$.

We mentioned the fact that $\mathcal{L}$ is a $\mathbf{Q}$-vector space. It was suggested by Euler that $\mathcal{L}$ is not a $\overline{\mathbf{Q}}$-vector space, and more precisely that for $\lambda \in \mathcal{L}$ and $\beta \in \overline{\mathbf{Q}}$, $\beta \notin \mathbf{Q}$, the number $\beta\lambda$ does not belong to $\mathcal{L}$. Writing $\lambda = \log\alpha$ and $\beta\lambda = \log(\alpha^\beta)$, the question is to prove that for any nonzero algebraic number α, any determination $\log\alpha$ of its logarithm (with the condition $\log\alpha \neq 0$, which needs to be added only if $\alpha = 1$), and any algebraic irrational β, the number α^β, which is defined as $\exp(\beta\log\alpha)$, is transcendental.

This is the seventh of Hilbert's problems. It was solved by A.O.Gel'fond and Th.Schneider in 1934. Their theorem can be stated as follows: *if λ_1, λ_2 are two elements of $\mathcal{L}$ which are linearly independent over $\mathbf{Q}$, then they are linearly independent over $\overline{\mathbf{Q}}$.* In other terms the quotient of two elements of $\mathcal{L}$ either is rational or else is transcendental.

An earlier transcendence result concerning $\mathcal{L}$ is due to Hermite and Lindemann: it says

$$\overline{\mathbf{Q}} \cap \mathcal{L} = \{0\}.$$

This means that *the equation* $\beta = \lambda$ *with* $\beta \in \overline{\mathbf{Q}}$ *and* $\lambda \in \mathcal{L}$ *has the only solution* $\beta = \lambda = 0$. A logarithm of an algebraic number cannot be algebraic unless it vanishes. If we write $\alpha = e^{\lambda}$, then the equation $\alpha = e^{\beta}$ with algebraic α and β has the only solution $(\alpha = 1,\ \beta = 0)$. This includes the transcendence of π (take for instance $\alpha = 1$, $\lambda = 2\pi i$), while the theorem of Gel'fond-Schneider includes the transcendence of e^{π} (again $\lambda = 2\pi i$, take $\beta = -i/2$, hence $\beta\lambda = \pi$ does not belong to $\mathcal{L}$).

The theorem of Baker generalizes at the same time the theorems of Hermite-Lindemann and Gel'fond-Schneider: *if* $\lambda_1, ..., \lambda_n$ *are* $\mathbf{Q}$*-linearly independent elements of* $\mathcal{L}$*, then the numbers* $1, \lambda_1, ..., \lambda_n$ *are linearly independent over* $\overline{\mathbf{Q}}$.

Our purpose is to discuss the following conjecture.

Conjecture. If $\lambda_1, ...\lambda_n$ *are* $\mathbf{Q}$*-linearly independent elements of* $\mathcal{L}$*, then they are algebraically independent.*

The conclusion means that for any nonzero polynomial P in n variables with rational coefficients, the number $P(\lambda_1, ..., \lambda_n)$ does not vanish. If that is true, then for any non constant polynomial P in n variables with algebraic coefficients, the number $P(\lambda_1, ..., \lambda_n)$ is transcendental. From this point of view, Baker's theorem is the very first step towards a proof of the conjecture of algebraic independence: it solves the problem for polynomials of degree 1 with algebraic coefficients.

We are presently very far from the goal. It is still not known that there exist two elements of $\mathcal{L}$ which are algebraically independent. We do not even know whether non trivial quadratic relations between elements of $\mathcal{L}$ can occur. We now discuss the problem of quadratic relations more thoroughly.

§2. Homogeneous quadratic relations.

The following open problem is known as the *four exponentials conjecture*: *if λ_1, λ_2, λ_3, λ_4 are nonzero elements of $\mathcal{L}$ which satisfy $\lambda_1\lambda_4 = \lambda_2\lambda_3$, then either λ_1/λ_3 is rational or λ_1/λ_2 is rational.* In terms of matrices, it means that a 2×2 matrix

$$\begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}$$

whose entries are in $\mathcal{L}$ and with vanishing determinant has either its rows linearly dependent over $\mathbf{Q}$ or its columns linearly dependent over $\mathbf{Q}$. The name of the conjecture arises from the following equivalent formulation: *if x_1, x_2 are $\mathbf{Q}$-linearly independent complex numbers and if also y_1, y_2 are $\mathbf{Q}$-linearly independent in $\mathbf{C}$, then one at least of the four numbers $e^{x_1y_1}$, $e^{x_1y_2}$, $e^{x_2y_1}$, $e^{x_2y_2}$ must be transcendental* (notice that a 2×2 matrix has zero determinant if and only if it can be written

$$\begin{pmatrix} x_1y_1 & x_1y_2 \\ x_2y_1 & x_2y_2 \end{pmatrix}$$

for some complex numbers x_1, x_2, y_1, y_2).

This question occurred for the first time after a work by Ramanujan on the quotient of consecutive highly composite numbers: for the proof of Ramanujan's claim that such a quotient is always a prime, Alaoglu and Erdős faced the problem of proving that a real number $t > 0$, such that ${p_1}^t \in \mathbf{Z}$ and ${p_2}^t \in \mathbf{Z}$ for two distinct primes p_1, p_2, must be an integer. An answer to this question is not yet known. Only a partial answer is known (one needs to add a further assumption ${p_3}^t \in \mathbf{Z}$ for a third prime p_3), which was provided by Siegel to Alaoglu and Erdős. It was part of the "folklore" in the 50's (according to Selberg also). This result of Siegel shows that Ramanujan's quotient is either a prime or else the product of two primes. In terms of matrices, it states that *a $d \times l$ matrix $(\lambda_{ij})_{1\leq i\leq d, 1\leq j\leq l}$ with entries in $\mathcal{L}$, whose rows are linearly independent over $\mathbf{Q}$, and whose columns are linearly independent over $\mathbf{Q}$, has* rank ≥ 2, *assuming $dl > d+l$.* The interesting cases for (d, l) are $(2, 3)$ and $(3, 2)$ (which amounts to the same by transposition) and this yields the following equivalent statement, known as the *six exponentials theorem*: *if x_1, x_2 are two $\mathbf{Q}$-linearly independent complex numbers and y_1, y_2, y_3 three $\mathbf{Q}$-linearly independent complex numbers, then one at least of the six numbers $e^{x_iy_j}$, $(i = 1, 2; j = 1, 2, 3)$ is transcendental.* The proof has first been published by S.Lang and K.Ramachandra.

We just mention that if we are looking for higher ranks, it is not sufficient to assume the $\mathbf{Q}$-linear independence of the rows and of the columns (consider for instance a matrix whose entries which are neither on the first row nor on the first column vanish: the rank is just 2). A sufficient condition is to assume that there is no non trivial relation

$$\sum_{i=1}^{d}\sum_{j=1}^{l} t_i s_j \lambda_{ij} = 0$$

with rational integers $t_1, ..., t_d, s_1, ..., s_l$. Under this hypothesis (in fact under a much weaker assumption) the rank of matrix is $\geq dl/(d+l)$.

We now come back to the four exponentials conjecture and investigate a couple of special interesting cases.

Remark 1 (due to Guy Diaz). Assuming the four exponentials conjecture, one deduces that *for $z \in \mathbf{C}$ with $|z| = 1$ and $z \neq \pm 1$, the number $e^{2\pi i z}$ is transcendental.*

This produces an interesting example of a curve which misses all algebraic points. A similar example (pointed out to me by F. Amoroso) of a curve, which is not a straight line nor a circle, and passes only through transcendental points (with a single exception: $z = i$) is $z = x + ie^x$, with $x \in \mathbf{R}$.

Proof. Assume $z \in \mathbf{C}$ satisfies $|z| = 1$ and $e^{2\pi i z} \in \overline{\mathbf{Q}}$. The number $\lambda = 2\pi i z$ belongs to $\mathcal{L}$, and its complex conjugate $\overline{\lambda} = -2\pi i \overline{z}$ also. From $z\overline{z} = 1$ one deduces $\lambda\overline{\lambda} = 4\pi^2$. The determinant of the matrix

$$\begin{pmatrix} \lambda & 2\pi i \\ -2\pi i & \overline{\lambda} \end{pmatrix}$$

vanishes. Since the entries are in $\mathcal{L}$, the four exponentials conjecture yields $\lambda \in 2\pi i\mathbf{Q}$, i.e. $z \in \mathbf{Q}$. Since $|z| = 1$, we conclude $z = \pm 1$.

Remark 2 (due to Daniel Bertrand). The next remark involves the modular invariant $j(\tau)$, which is an analytic function in the upper half plane $\mathcal{H} = \{\tau \in \mathbf{C}, \Im\tau > 0\}$ and satisfies

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau) \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

any matrix with rational integer entries of determinant $+1$. From the periodicity relation $j(\tau + 1) = j(\tau)$ follows that there is an analytic function J

in $D(0,1)-\{0\}=\{q\in\mathbf{C}, 0<|q|<1\}$ such that $J(e^{2\pi i\tau})=j(\tau)$ for $\tau\in\mathcal{H}$. The function j is uniquely determined (up to an additive constant) by the above properties together with the condition that J has a simple pole at 0 of residue 1. The Laurent expansion of J at 0 is

$$J(q)=\frac{1}{q}+744+196884q+\cdots+c(n)q^n+\cdots$$

with positive integers $c(n)$.

The connection with our subject is the following: assuming the four exponentials conjecture, it follows that J *is injective on the set of algebraic numbers in* $D(0,1)-\{0\}$.

Proof (following D. Bertrand). Assume $J(q_1)=J(q_2)$ with algebraic q_1, q_2 satisfying $0<|q_k|<1$, $(k=1,\,2)$. Let τ_1 and τ_2 in $\mathcal{H}$ satisfy $q_k=e^{2\pi i\tau_k}$. Then $j(\tau_1)=j(\tau_2)$. From the properties of j one knows that there exists a matrix

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in \mathrm{SL}_2(\mathbf{Z})$$

with

$$\tau_2=\frac{a\tau_1+b}{c\tau_1+d}.$$

If we define $\lambda_k=2\pi i\tau_k$, $(k=1,2)$, then $\lambda_k\in\mathcal{L}$ and

$$\det\begin{pmatrix}\lambda_2 & a\lambda_1+b2\pi i\\ 2\pi i & c\lambda_1+d2\pi i\end{pmatrix}=0.$$

Since $\tau_2\in\mathcal{H}$, we have $\tau_2\notin\mathbf{Q}$, and $\lambda_2\notin 2\pi i\mathbf{Q}$. From the four exponentials conjecture follows that λ_2 and $a\lambda_1+b2\pi i$ are $\mathbf{Q}$-linearly dependent. Hence 1, τ_1, τ_2 are $\mathbf{Q}$-linearly dependent:

$$m\tau_2=n\tau_1+l$$

with $(m,n,l)\in\mathbf{Z}^3$, $(m,n,l)\neq(0,0,0)$. Replace τ_2 by $(a\tau_1+b)/(c\tau_1+d)$. We get a quadratic relation for τ_1. However since $q_1=e^{2\pi i\tau_1}$ is algebraic and τ_1 is irrational, Gel'fond-Schneider theorem shows that τ_1 is transcendental. Therefore our quadratic relation is trivial, and we deduce $\tau_2=\tau_1+b$ which gives $q_2=q_1$, as asserted.

As far as these functions j and J are concerned, it was known for a long time (due to Schneider) that $j(\tau)$ *is transcendental when* τ *is algebraic and* *not quadratic* (while from the theory of complex multiplication, one knows that $j(\tau)$ is algebraic for τ quadratic in $\mathcal{H}$). Only last year (1995) it has been proved by K.Barré-Sirieix, G.Diaz, F.Gramain and G.Philibert that $J(q)$ *is transcendental for algebraic* q *with* $0 < |q| < 1$. A few months ago (1996), Y.Nesterenko extended their method thanks to a zero estimate of his own and got a result of algebraic independence on the values of Eisenstein series, which implies that *the three numbers* π, e^π *and* $\Gamma(1/4)$ *are algebraically independent.* It was not known, before, that π and e^π are algebraically independent (but it was known for π and $\Gamma(1/4)$, due to Chudnovsky). Effective results of diophantine approximation for these numbers have also been produced by Nesterenko as well as by P.Philippon.

We now come back to our main concern which is the question of existence of quadratic relations between logarithms of algebraic numbers. One of the first results in this direction goes back to the early 70's, due to Brownawell and Waldschmidt. We call it the "four exponentials theorem in transcendence degree 1": *if* λ_1, λ_2, λ_3, λ_4 *are nonzero elements of* $\mathcal{L}$ *with* $\lambda_1/\lambda_2 \notin \mathbf{Q}$ *and* $\lambda_1/\lambda_3 \notin \mathbf{Q}$, *and if the field* $\mathbf{Q}(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ *has transcendence degree* 1, *then* $\lambda_1\lambda_4 \neq \lambda_2\lambda_3$.

The *transcendence degree* of a field is the maximal number of algebraically independent elements it contains. An algebraic number field has transcendence degree 0. As soon as a field contains a transcendental element (for instance a nonzero logarithm of an algebraic number), its transcendence degree is ≥ 1.

Here is a generalization of the four exponentials theorem in transcendence degree 1. It is a joint work with D.Roy and has been announced in 1995 in Proc. Japan Acad. Sci.

Theorem 1. *Let* $\lambda_1, ..., \lambda_n$ *be elements of* $\mathcal{L}$ *and let* Q *be a nonzero homogeneous quadratic form with rational coefficients. Assume that the transcendence degree of the field* $\mathbf{Q}(\lambda_1, ..., \lambda_n)$ *is* 1, *and that* $Q(\lambda_1, ..., \lambda_n) = 0$. *Then there is a vector subspace* V *of* $\mathbf{C}^n$, *rational over* $\mathbf{Q}$, *which is contained in the set of zeroes of* Q *and contains* $(\lambda_1, ..., \lambda_n)$.

When $K \subset C$ are two fields, a vector subspace of C^n is said to be *rational over* K if it can be defined by homogeneous linear equations with coefficients in K. An equivalent definition is to say that it has a basis (as a C-vector space) whose elements belong to K^n.

In order to deduce from theorem 1 the four exponentials theorem in transcendence degree 1, we take $n = 4$ and $Q(X_1, X_2, X_3, X_4) = X_1X_4 - X_2X_3$.

For $(\lambda, \mu) \in \mathbf{Q}^2$, $(\lambda, \mu) \neq (0,0)$, the subspace

$$\{(z_1, z_2, z_3, z_4) \in \mathbf{C}^4; \lambda z_1 = \mu z_2, \lambda z_3 = \mu z_4\}$$

of $\mathbf{C}^4$ is of dimension 2 over $\mathbf{C}$ (it is a complex plane) which is contained in the hypersurface defined by Q. Moreover this plane depends only on the class $(\lambda : \mu)$ of (λ, μ) in the projective line $\mathbf{P}_1(\mathbf{Q})$. Similarly the plane

$$\{(z_1, z_2, z_3, z_4) \in \mathbf{C}^4; \lambda z_1 = \mu z_3, \lambda z_2 = \mu z_4\}$$

is contained in the set of zeroes of the quadratic form Q. Clearly it suffices to prove that any vector subspace of $\mathbf{C}^4$ which is contained in the hypersurface $Q(z) = 0$ is contained in one of these planes.

Lemma. *Let C be a field with infinitely many elements, K be a subfield of C and V a vector subspace of C^4, which is rational over K. Assume $z_1 z_4 = z_2 z_3$ for all $(z_1, z_2, z_3, z_4) \in V$. Then there exists $(\lambda : \mu) \in \mathbf{P}_1(K)$ such that V is included either in the plane*

$$W_{(\lambda:\mu)} = \{(z_1, z_2, z_3, z_4) \in C^4; \lambda z_1 = \mu z_2, \lambda z_3 = \mu z_4\}$$

or in the plane

$$W'_{(\lambda:\mu)} = \{(z_1, z_2, z_3, z_4) \in C^4; \lambda z_1 = \mu z_3, \lambda z_2 = \mu z_4\}.$$

Proof. Since the field C has infinitely many elements, a subspace of C^4 is not the union of finitely many proper subspaces. The lemma is clear if V is contained in one of the four planes $W_{(0:1)}$, $W_{(1:0)}$, $W'_{(0:1)}$, $W'_{(1:0)}$. Otherwise, there exists $v = (a, b, c, d) \in V$ such that $abcd \neq 0$. Since $ad = bc$, we have $(b : a) = (d : c)$ and $(c : a) = (d : b)$. We assume that V is not contained in $W_{(b:a)}$ nor in $W'_{(c:a)}$ and we shall get a contradiction. From our assumption we deduce that there exists $v' = (a', b', c', d')$ in V which does not belong to

$$W_{(0:1)} \cup W_{(1:0)} \cup W'_{(0:1)} \cup W'_{(1:0)} \cup W_{(b:a)} \cup W'_{(c:a)}.$$

In particular $a'b'c'd' \neq 0$. We have $xv + x'v' \in V$ for all (x, x') in C^2, hence $Q(xv + x'v') = 0$:

$$(ad - bc)x^2 + (a'd - bc' - b'c + ad')xx' + (a'd' - b'c')x'^2 = 0$$

for all $(x,x')\in C^2$. We deduce $ad=bc$, $a'd'=b'c'$ and $a'd+ad'=bc'+b'c$. Therefore

$$(cd'-c'd)(bd'-b'd)=dd'(a'd-bc'-b'c+ad')=0.$$

Hence one at least of the two numbers $cd'-c'd$, $bd'-b'd$ vanish. If $cd'-c'd=0$ then

$$\frac{a}{b}=\frac{c}{d}=\frac{c'}{d'}=\frac{a'}{b'},$$

and $v'\in W_{(b:a)}$. Similarly If $bd'-b'd=0$ then

$$\frac{a}{c}=\frac{b}{d}=\frac{b'}{d'}=\frac{a'}{c'},$$

and $v'\in W'_{(c:a)}$. In both cases we get a contradiction.

Now we use the assumption that V is rational over K: there is a basis $(e_1,\ldots,e_d)$ of V (with $d\le 2$) with $e_i=(e_{i1},e_{i2},e_{i3},e_{i4})\in K^4$. If V is included in $W_{(\lambda:\mu)}$ for some $(\lambda:\mu)\in\mathbf{P}_1(C)$, then the system of equations

$$xe_{i1}=ye_{i2},\quad xe_{i3}=ye_{i4},\qquad (i=1,\ldots,d)$$

has a non trivial solution $(x,y)\in C^2$, hence it has a non trivial solution $(x,y)\in K^2$, and therefore V is included in $W_{(\lambda:\mu)}$ for some $(\lambda:\mu)\in\mathbf{P}_1(K)$. The same arguments works for $W'_{(\lambda:\mu)}$.

The lemma plainly follows.

Remark. It would be very interesting to extend the theorem to non homogeneous quadratic polynomials. Even the case of the polynomial $X_1X_2-X_3$ would have nice consequences: take $\lambda_1=\lambda_2=\pi i$ and $\lambda_3\in\mathcal{L}$. It would follow that e^{π^2} is transcendental, which is not yet known. More generally the transcendence of e^{λ^2} for $\lambda\in\mathcal{L}$, $\lambda\neq 0$ would follow. It is only known that one of the two numbers e^{λ^2}, e^{λ^3} is transcendental (Brownawell and the author).

More generally one expects that for $\lambda\in\mathcal{L}$, $\lambda\neq 0$, the two numbers λ and e^{λ^2} should be algebraically independent. Another open problem is the algebraic independence of the two numbers λ and $e^{\beta\lambda}$ for $\lambda\in\mathcal{L}$, $\lambda\neq 0$ and β irrational quadratic. Nesterenko's theorem on Eisenstein series solves this problem when $\lambda=\pi i$ and β is real quadratic: *the two numbers π, $e^{\pi\sqrt{D}}$ (for D any positive integer) are algebraically independent.*

§3. Elliptic analogues.

There are several elliptic analogues to the four exponentials conjecture. We start with the simplest one. Let $\wp$ be a Weierstrass elliptic function with algebraic invariants g_2, g_3:

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

An elliptic logarithm is a complex number u which either is a pole of $\wp$, or else satisfies $\wp(u) \in \overline{\mathbf{Q}}$. The set $\mathcal{L}_E$ (where the index E stands for the elliptic curve) is a $\mathbf{Z}$-module. In fact it is a module over the ring $\mathrm{End}E$ of endomorphisms of the elliptic curve E associated to $\wp$, and also a vector space over field $\mathrm{End}^0E = \mathrm{End}E \otimes_{\mathbf{Z}} \mathbf{Q}$.

The *pure elliptic four exponentials conjecture* asserts that *for u_1, u_2, u_3, u_4 in $\mathcal{L}_E$ with u_1, u_2 linearly independent over* $\mathrm{End}E$ *and also u_1, u_3 linearly independent over* $\mathrm{End}E$*, the determinant of the matrix*

$$\begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$$

does not vanish.

There is also a mixed four exponentials conjecture which deals with the product of the multiplicative group by an elliptic curve: consider a matrix

$$\begin{pmatrix} \lambda_1 & u_1 \\ \lambda_2 & u_2 \end{pmatrix}$$

where λ_1, λ_2 are $\mathbf{Q}$-linearly independent elements of $\mathcal{L}$ and u_1, u_2 are non zero elements of $\mathcal{L}_E$. Then the conjecture is that *the determinant* $\lambda_1 u_2 - \lambda_2 u_1$ *does not vanish.* Here there is one case where the problem is solved, namely when one of λ_j is $2\pi i$ and when (u_1, u_2) is a basis (ω_1, ω_2) of the periodic lattice. Indeed the assumption $(g_2, g_3) \in \overline{\mathbf{Q}}^2$ implies that the number $j(\omega_2/\omega_1)$ is algebraic, hence, according to Barré-Sirieix, Diaz, Gramain and Philibert, the number $e^{2\pi i\omega_2/\omega_1}$ is transcendental.

To conclude, we state a further result of our joint work with D.Roy, which is the elliptic analogue of the previous theorem 1 in the so-called CM case.

Theorem 2. *Let $\wp$ be a Weierstrass elliptic function with algebraic invariants g_2, g_3 and with* $\mathrm{End}E \neq \mathbf{Z}$. *Let $u_1, ..., u_n$ be elements of $\mathcal{L}_E$ and $Q \in \mathbf{Q}[X_1, ..., X_n]$ be a homogeneous quadratic form such that $Q(u_1, ..., u_n) = 0$. Assume that the field $\mathbf{Q}(u_1, ..., u_n)$ has transcendence degree 1. Then $(u_1, ..., u_n)$ belongs to a vector subspace of $\mathbf{C}^n$, which is rational over the field* End^0E, *and is contained in the set of zeros of Q.*

REFERENCES

This lecture is based on three joint papers with Damien ROY:

Quadratic relations between logarithms of algebraic numbers, Proc. Japan Acad. Sci., Sér. A, **71** (1995), 151–153.

Approximation diophantienne et indépendance algébrique de logarithmes, submitted (37 pp.).

Simultaneous approximation and algebraic independence, submitted (48 pp.). Rapports CICMA Reports, 1996-05.

A survey on this subject has been recently written by M. LAURENT :

New methods in algebraic independence, Proc. Conf. Number Theory Eger 1996, to appear.

Further references concerning modular functions are given in the following two lectures of the author:

Sur la nature arithmétique des valeurs de fonctions modulaires, Sém. Bourbaki 49ème année (1996/97), N° 824; to appear in Astérisque, Soc. Math. France.

Transcendance et indépendance algébrique de valeurs de fonctions modulaires, submitted.

Michel Waldschmidt
Institut de Mathématiques de Jussieu
Problèmes Diophantiens Case 247
4, place Jussieu
F–75252 PARIS CEDEX 05
e-mail: `miw@math.jussieu.fr`
internet: `http://www.math.jussieu.fr/~miw`