Astérisque

DAVID WILLIAM MASSER

Transcendence and abelian functions

Astérisque, tome 24-25 (1975), p. 177-182

<http://www.numdam.org/item?id=AST_1975__24-25__177_0>

Société Mathématique de France
Astérisque 24-25 (1975)

TRANSCENDENCE AND ABELIAN FUNCTIONS

by

David William MASSER

-:-:-:-

I will first describe the results in the special case of elliptic functions. Let g_2, g_3 be algebraic numbers with $g_2^3 \neq 27 g_3^2$, and let $\wp(z)$ be the Weierstrass elliptic function satisfying the differential equation :

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2 \wp(z) - g_3 \quad . \tag{*}$$

This function is doubly periodic with a lattice Λ of periods which are also poles. We define an algebraic point of $\wp(z)$ as a complex number u such that either u is in Λ or $\wp(u)$ is an algebraic number. The ring $\mathbb{E}$ of complex multiplications of $\wp(z)$ is the ring of complex numbers σ such that $\sigma\Lambda \subseteq \Lambda$. Clearly $\mathbb{E} \supseteq \mathbb{Z}$, and for general g_2, g_3 we have $\mathbb{E} = \mathbb{Z}$; otherwise $\mathbb{E}$ is an order of a complex quadratic extension $\mathbb{K}$ of the rational field $\mathbb{Q}$. It is not hard to prove that the set of algebraic points of $\wp(z)$ is an $\mathbb{E}$-module. Accordingly it was conjectured by Coates that algebraic points of $\wp(z)$ are linearly independent over the field $\mathbb{A}$ of algebraic numbers if and only if they are linearly independent over $\mathbb{E}$.

I have proved this conjecture when $\mathbb{E} \neq \mathbb{Z}$, and the following theorem is an essential tool.

THEOREM 1. - Let $u_1, \dots, u_m$ be algebraic points of $\wp(z)$ that are linearly independent over $\mathbb{E}$ ($\neq \mathbb{Z}$). Then given $\varepsilon > 0$ there is an effectively computable constant $C > 0$ depending only on ε, $u_1, \dots, u_m$ and $\wp(z)$ such that

$$|\sigma_1 u_1 + \dots + \sigma_m u_m| > C\, e^{-H^{\varepsilon}}$$

for any algebraic numbers $\sigma_1, \dots, \sigma_m$ of $\mathbb{E}$, not all zero, of heights at most H .

With this we can prove the following generalization of the conjecture which incorporates the number 1 into the basic linear form.

THEOREM 2. - Let $u_1, \dots, u_m$ be algebraic points of $\wp(z)$ that are linearly independent over $\mathbb{E}$ ($\neq \mathbb{Z}$). Then 1 , $u_1, \dots, u_m$ are linearly independent over $\mathbb{A}$.

In particular, each u_i and each ratio u_i/u_j is transcendental ; in fact these special cases were obtained by Schneider in [2] for general $\mathbb{E}$. The quantitative version of theorem 1 can be used in conjunction with the finite basis theorem of Mordell-Weil to give a new proof of Siegel's theorem for elliptic curves with complex multiplication. For example, if k is a non-zero rational integer, the curves

$$y^2 = x^3 + k \quad , \quad y^2 = x^3 + kx$$

have only finitely many integral points.

Although this proof does not use the inequality of Thue-Siegel-Roth, it remains ineffective in character because there is no effective way of constructing the basis whose existence is asserted by the result of Mordell-Weil.

To generalize all this to abelian functions we proceed as follows. Let Λ be a lattice in $\mathbb{C}^n$ satisfying certain relations of Riemann. If it is non-degenerate in a certain sense, the field $\mathfrak{F}$ of functions meromorphic on $\mathbb{C}^n$ containing Λ in its lattice of periods is of transcendence degree n over $\mathbb{C}$. Thus we may write

$$\mathfrak{F} = \mathbb{C}(A_o, A_1, \dots, A_n)$$

where $A_1, \dots, A_n$ are algebraically independent and A_o is integral over the ring $\mathbb{C}[A_1, \dots, A_n]$. We express this dependence by a polynomial relation

$$F(A_o, A_1, \dots, A_n) = 0 \quad .$$

For example, if $n = 1$ we can take $A_1 = \wp$, $A_o = \wp'$ and F is given by (*). The analogue of the condition that g_2, g_3 are algebraic numbers is imposed as follows. The partial derivatives $\partial/\partial Z_i$ map $\mathfrak{F}$ to itself, and so we can write

$$G(A_1, \dots, A_n)\, \partial A_j/\partial Z_i = G_{ij}(A_o, A_1, \dots, A_n) \quad (1 \leq i \leq n,\ 0 \leq j \leq n)$$

after taking a common denominator and clearing this of the function A_o. We say that $\mathfrak{F}$ is algebraically defined if

a) $A_1, \dots, A_n$ are holomorphic at the origin $\underline{0}$ and take algebraic values there,

b) F, G, G_{ij} have algebraic coefficients,

c) If we write $B(\underline{Z}) = G(A_1(\underline{Z}), \dots, A_n(\underline{Z}))$ then $B(\underline{0}) \neq 0$.

We call a vector $\underline{u}$ of $\mathbb{C}^n$ an algebraic point of $\mathfrak{F}$ if

d) $A_1, \dots, A_n$ are holomorphic at $\underline{u}$ and take algebraic values there,

e) $B(\underline{u}) \neq 0$.

Once again we define $\mathbb{E}$ as the ring of matrices of $GL_n(\mathbb{C})$ that take the period lattice Λ into itself. It is no longer true that algebraic points form a

$\mathbb{E}$-module, because of the denominator $B(\underline{Z})$; however, this statement is almost always true. The conjecture extending that of Coates would assert that algebraic points of $\mathfrak{J}$ are linearly independent over $M_n(\mathbb{A})$ if and only if they are linearly independent over $\mathbb{E}$, where $M_n(\mathbb{A})$ denotes the ring of $n \times n$ matrices with algebraic entries.

Our methods only succeed when $\mathfrak{J}$ has complex multiplication of the type discussed by Shimura. This is when $\mathbb{E}$ is isomorphic to an order $\mathbb{L}$ of an algebraic number field $\mathbb{F}$ of degree $2n$ over $\mathbb{Q}$. It is convenient to make this isomorphism explicit by diagonalizing $\mathbb{E}$. There are n monomorphisms $\psi_i : \mathbb{F} \to \mathbb{C}$ $(1 \leq i \leq n)$ such that the diagonal matrix $D(\sigma)$ of $\mathbb{E}$ corresponding to a number σ of $\mathbb{L}$ is given by

$$D(\sigma) = \operatorname{diag}(\sigma^{\psi_1}, \ldots, \sigma^{\psi_n}) .$$

The next result generalizes Theorem 1 .

THEOREM 3. - Let $\underline{u}_1, \ldots, \underline{u}_m$ be algebraic points of $\mathfrak{J}$ that are linearly independent over $\mathbb{E}$ $(\approx \mathbb{L})$. Then given $\varepsilon > 0$ there is an effectively computable constant $C > 0$ depending only on ε , $\underline{u}_1, \ldots, \underline{u}_m$, and $\mathfrak{J}$ such that

$$|D(\sigma_1)\,\underline{u}_1 + \ldots + D(\sigma_m)\,\underline{u}_m| > C\, e^{-H^{\varepsilon}}$$

for any algebraic numbers $\sigma_1, \ldots, \sigma_m$ of $\mathbb{L}$, not all zero, with heights at most H .

This enables us to give a new proof of Siegel's Theorem for any curve whose Jacobian variety has Shimura complex multiplication. An example is

$$a x^p + b y^q + c = 0$$

where a , b , c are nonzero rational integers and p, q are different primes.

Once again the estimates would all become effective if the theorem of Mordell-Weil for abelian varieties could be made effective.

Finally Theorem 2 can be generalized by introducing the vector $\underline{v} = (1, 1, \dots, 1)$.

THEOREM 4. - Let $\underline{u}_1, \dots, \underline{u}_m$ be algebraic points linearly independent over $\mathbb{E}$ ($\approx \mathbb{L}$). Then the vectors $\underline{v}, \underline{u}_1, \dots, \underline{u}_m$ are linearly independent over the set of non-zero diagonal matrices of $M_n(\mathbb{A})$.

In other words, if $R, S_1, \dots, S_m$ are diagonal matrices of $M_n(\mathbb{A})$, not all zero, the vector

$$R\underline{v} + S_1\underline{u}_1 + \dots + S_m\underline{u}_m$$

does not vanish. This clearly gives the transcendence of the vectors $\underline{u}_i$ (i. e. the transcendence of at least one of their components) ; this had been proved for general $\mathbb{E}$ by Lang in [1]. More interestingly, we can separate components by taking the matrix coefficients suitably singular. For example, when $m = 1$ we can take for algebraic α

$$R = \text{diag}(\alpha, 0, \dots, 0) \qquad S_1 = \text{diag}(1, 0, \dots, 0) \quad ;$$

this implies the transcendence of the first component of $\underline{u}_1$ (and so obviously that of each component). Similarly, the choice $R = 0$ and

$$S_i = \text{diag}(\alpha_i, 0, \dots, 0)$$

for algebraic α_i gives the linear independence over $\mathbb{A}$ of the first components of $\underline{u}_1, \dots, \underline{u}_m$.

-:-:-:-

REFERENCES

[1] S. LANG. - Introduction to Transcendental Numbers. Addison-Wesley, Reading, (1966).

[2] T. SCHNEIDER. - Einführung in die transzendenten Zahlen. Springer-Verlag, Berlin, (1957).

-:-:-:-

David William MASSER
University of Nottingham
Department of Mathematics
University Park
NOTTINGHAM NG7 2RD