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>
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:

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

(*)

This function is doubly periodic with a lattice $\Lambda$ 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 $\Lambda$ or $\wp(u)$ is an algebraic number. The ring $\mathbb{E}$ of complex multiplications of $\wp(z)$ is the ring of complex numbers $\sigma$ such that $\sigma \Lambda \leq \Lambda$. Clearly $\mathbb{E} \supset \mathbb{Z}$, 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 $u_1, \ldots, u_m$ be algebraic points of $\mathcal{P}(z)$ 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 $\varepsilon$, $u_1, \ldots, u_m$ and $\mathcal{P}(z)$ such that

$$\left| \sum_{i=1}^{m} \sigma_i u_i \right| > C e^{-H^\varepsilon}$$

for any algebraic numbers $\sigma_1, \ldots, \sigma_m$ 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 $u_1, \ldots, u_m$ be algebraic points of $\mathcal{P}(z)$ that are linearly independent over $\mathbb{E} (\neq \mathbb{Z})$. Then $1, u_1, \ldots, u_m$ 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

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

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 \( \Lambda \) be a lattice in \( \mathbb{C}^n \) satisfying certain relations of Riemann. If it is non-degenerate in a certain sense, the field \( \mathcal{F} \) of functions meromorphic on \( \mathbb{C}^n \) containing \( \Lambda \) in its lattice of periods is of transcendence degree \( n \) over \( \mathbb{C} \). Thus we may write

\[
\mathcal{F} = \mathbb{C}(A_0, A_1, \ldots, A_n)
\]

where \( A_1, \ldots, A_n \) are algebraically independent and \( A_0 \) is integral over the ring \( \mathbb{C}[A_1, \ldots, A_n] \). We express this dependence by a polynomial relation

\[
F(A_0, A_1, \ldots, A_n) = 0.
\]

For example, if \( n = 1 \) we can take \( A_1 = \rho \), \( A_0 = \rho' \) and \( F \) is given by (1).

The analogue of the condition that \( g^1, \ldots, g^n \) are algebraic numbers is imposed as follows. The partial derivatives \( \partial / \partial Z_i \) map \( \mathcal{F} \) to itself, and so we can write

\[
G(A_1, \ldots, A_n) \partial A_j / \partial Z_i = G_{ij}(A_0, A_1, \ldots, A_n) \quad (1 \leq i \leq n, 0 \leq j \leq n)
\]

after taking a common denominator and clearing this of the function \( A_0 \). We say that \( \mathcal{F} \) is algebraically defined if

a) \( A_1, \ldots, A_n \) are holomorphic at the origin \( 0 \) and take algebraic values there,

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

c) If we write \( B(Z) = G(A_1(Z), \ldots, A_n(Z)) \) then \( B(0) \neq 0 \).

We call a vector \( u \) of \( \mathbb{C}^n \) an algebraic point of \( \mathcal{F} \) if

d) \( A_1, \ldots, A_n \) are holomorphic at \( u \) and take algebraic values there,

e) \( B(u) \neq 0 \).

Once again we define \( \mathbb{E} \) as the ring of matrices of \( GL_n(\mathbb{C}) \) that take the period lattice \( \Lambda \) into itself. It is no longer true that algebraic points form a
$$\mathcal{E}$$-module, because of the denominator $B(Z)$; however, this statement is almost always true. The conjecture extending that of Coates would assert that algebraic points of $\mathfrak{F}$ are linearly independent over $M_n(\mathbb{A})$ if and only if they are linearly independent over $\mathcal{E}$, where $M_n(\mathbb{A})$ denotes the ring of $n \times n$ matrices with algebraic entries.

Our methods only succeed when $\mathfrak{F}$ has complex multiplication of the type discussed by Shimura. This is when $\mathcal{E}$ is isomorphic to an order $\mathcal{O}_L$ of an algebraic number field $\mathbb{F}$ of degree $2n$ over $\mathbb{Q}$. It is convenient to make this isomorphism explicit by diagonalizing $\mathcal{E}$. There are $n$ monomorphisms

$$\psi_i : \mathbb{F} \to \mathbb{C} \ (1 \leq i \leq n)$$

such that the diagonal matrix $D(\sigma)$ of $\mathcal{E}$ corresponding to a number $\sigma$ of $\mathcal{O}_L$ is given by

$$D(\sigma) = \text{diag}(\psi_1(\sigma), \ldots, \psi_n(\sigma))$$

The next result generalizes Theorem 1.

**Theorem 3.** Let $u_1, \ldots, u_m$ be algebraic points of $\mathfrak{F}$ that are linearly independent over $\mathcal{E}$ ($\cong \mathcal{O}_L$). Then given $\varepsilon > 0$ there is an effectively computable constant $C > 0$ depending only on $\varepsilon$, $u_1, \ldots, u_m$, and $\mathfrak{F}$ such that

$$|D(\sigma_1)u_1 + \ldots + D(\sigma_m)u_m| > C e^{-H^\varepsilon}$$

for any algebraic numbers $\sigma_1, \ldots, \sigma_m$ of $\mathcal{O}_L$, 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

$$ax^p + by^q + c = 0$$

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 \( \mathbf{v} = (1, 1, \ldots, 1) \).

**THEOREM 4.** - Let \( u_1, \ldots, u_m \) be algebraic points linearly independent over \( E \). Then the vectors \( \mathbf{v}, u_1, \ldots, u_m \) are linearly independent over the set of non-zero diagonal matrices of \( M_n(A) \).

In other words, if \( R, S_1, \ldots, S_m \) are diagonal matrices of \( M_n(A) \), not all zero, the vector

\[
R \mathbf{v} + S_1 u_1 + \ldots + S_m u_m
\]

does not vanish. This clearly gives the transcendence of the vectors \( u_i \) (i.e. the transcendence of at least one of their components); this had been proved for general \( E \) 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 \( a \)

\[
R = \text{diag}(a, 0, \ldots, 0) \quad S_1 = \text{diag}(1, 0, \ldots, 0)
\]

this implies the transcendence of the first component of \( u_1 \) (and so obviously that of each component). Similarly, the choice \( R = 0 \) and

\[
S_i = \text{diag}(\alpha_i, 0, \ldots, 0)
\]

for algebraic \( \alpha_i \) gives the linear independence over \( A \) of the first components of \( u_1, \ldots, u_m \).
REFERENCES


---

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