D. W. MASSER

On quasi-periods of abelian functions with complex multiplication

Mémoires de la S. M. F. 2e série, tome 2 (1980), p. 55-68
<http://www.numdam.org/item?id=MSMF_1980_2_2__55_0>

SOCIÉTÉ MATHEMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 55-68

ON QUASI-PERIODS OF ABELIAN FUNCTIONS WITH COMPLEX MULTIPLICATION

by

D. W. MASSER

1. INTRODUCTION

Let $\mathcal{L}$ be an algebraically presented lattice in $\mathbb{C}^2$ in the sense of [6], and let $\theta_0(\underline{z}),\ldots,\theta_n(\underline{z})$ be theta functions on $\mathbb{C}^2$ which give an analytic isomorphism from the torus $\mathbb{C}^2/\mathcal{L}$ to an abelian variety A in projective space. As in [6], we may suppose that $\theta_0(\underline{0}) \neq 0$ and that the quotients $f_i(\underline{z}) = \theta_i(\underline{z})/\theta_0(\underline{z})$ $(1 \leq i \leq n)$ are abelian functions whose Taylor expansions about $\underline{z} = \underline{0}$ have algebraic coefficients. Let $g = g(\underline{z})$ be a quasi-periodic function in the sense of [5], analytic at $\underline{z} = \underline{0}$, whose Taylor expansion about $\underline{z} = \underline{0}$ also has algebraic coefficients. Thus the quasi-periods

$$\eta(g,\underline{\omega}) = g(\underline{z}+\underline{\omega}) - g(\underline{z}) \tag{1}$$

are independent of $\underline{z}$ for each $\underline{\omega}$ in $\mathcal{L}$. The main result of [5] states that if A is simple, g is not abelian, and $\underline{\omega}$ is non-zero, then $\eta = \eta(g,\underline{\omega})$ is transcendental.

The methods of [5] can also be used in a much easier way to prove that $\eta + \alpha\pi$ is either zero or transcendental for any algebraic number α. Presumably $\eta + \alpha\pi$ is in fact always transcendental in these circumstances. However, not even the analogue [4] of this result for the product of two elliptic curves has been proved in general. In this paper we resolve the problem when A has many complex multiplications in the sense of [6] and [7]. We prove the following theorem.

Theorem : Suppose A is simple and has many complex multiplications. Then if g is not abelian and ω is non-zero, the number $\eta(g, \underline{\omega}) + \alpha(2\pi i)$ is transcendental for any algebraic number α.

From the example given in [5] it is easy to deduce the following linear independence property of special values of the classical beta function B(x,y). This answers a question raised in [5].

Corollary : As r, s run over all positive integers the numbers $B(r/5, s/5)$ span a vector space of dimension 6 over the field of algebraic numbers.

Another consequence, obtained by taking g as a linear function, is the transcendence in dimension 2 of the expressions $p(\tau, \Phi)$ introduced by Shimura in his study [8] of algebraic relations between periods. The corresponding result in dimension 1 follows from the classical theorems of Schneider.

The proof of our Theorem relies on some distribution properties of certain division fields associated with A. These will be discussed in the next section. After that we shall give the main transcendence proof. But first we set up some preliminaries.

Using elementary specialization arguments on Fourier series, it is not too difficult to establish the existence of a theta function $\theta(\underline{z})$ with $\theta(\underline{0}) \neq 0$, non-degenerate in the sense of [9], whose Taylor expansion about $\underline{z} = \underline{0}$ has coefficients in an algebraic number field. This will be convenient (but not essential) for later use. We shall assume that the endomorphism ring of A is isomorphic to the ring of integers I of a totally imaginary quadratic extension K of a real quadratic field K_0. This assumption involves no loss of generality, as we can always replace $\mathcal{L}$ by an isogenous lattice (cf. [7] p.59). After strongly normalizing [2], we obtain embeddings φ_1, φ_2 of K into $\mathbb{C}$, inducing different embeddings of K_0 into $\mathbb{C}$, such that for any σ in I the corresponding endomorphism is represented in $\mathbb{C}^2$ by mapping $\underline{z} = (z_1, z_2)$ to $\underline{\sigma z} = (\sigma^{\varphi_1} z_1, \sigma^{\varphi_2} z_2)$. From now until the end of section 2 we fix an algebraic number field F, containing all the conjugates of K, such that the Taylor expansions of $f_1(\underline{z}), \ldots, f_n(\underline{z})$ and $\theta(\underline{z})$

about $\underline{z} = \underline{0}$ have coefficients in F.

Next, we suppose $f_1(\underline{z}),\ldots,f_n(\underline{z})$ to have been replaced by sufficiently general linear combinations of themselves with coefficients in F. This preserves the embedding property into projective space, and allows us to assume the following additional facts. Firstly, the Jacobian matrix of $f_1(\underline{z})$, $f_2(\underline{z})$ at $\underline{z} = \underline{0}$ is non-singular, so that in particular these functions are algebraically independent, and secondly, the functions $f_1(\underline{z}),\ldots,f_n(\underline{z})$ are all integral over the ring $F[f_1(\underline{z}),f_2(\underline{z})]$ (cf. [3] p.5, Remark 2.7).

Finally, we fix throughout the paper elements α_1, α_2, α_3, α_4 of an integral basis of K over the rational field $\mathbb{Q}$, and if d is the discriminant of K_0 we put $\alpha_0 = \sqrt{d}$. For α in K we denote by $Tr(\alpha)$, $N(\alpha)$ the trace and norm respectively of α from K to $\mathbb{Q}$. We write $\underline{\alpha} = (\alpha^{\varphi_1}, \alpha^{\varphi_2})$, and we multiply vectors of $\mathbb{C}^2$ componentwise, as in [6] .

2. DIVISION FIELDS

For a prime $\ell > 2$ we define F_ℓ as the field generated over F by the numbers $f_i(\underline{\omega}/\ell)$ $(1 \leq i \leq n)$ as $\underline{\omega}$ runs over all periods of $\mathcal{L}$ such that $\theta_0(\underline{\omega}/\ell) \neq 0$. It is easily seen that F_ℓ is a Galois extention of F. It is known from class field theory and the results of [7] that for all sufficiently large ℓ the field F_ℓ contains $M_\ell = F(e^{2\pi i/\ell})$ and has degree at most $c\ell^3$ for some c independent of ℓ . In fact it is convenient for us to derive elementary proofs of these statements in the course of obtaining the required distribution properties of F_ℓ .

We shall also need the less elementary fact that the degree of F_ℓ exceeds $c'\ell^3$ for some $c' > 0$ independent of ℓ. During the conference Professor Shimura showed me how to deduce this from the results of [7], and I am grateful for his permission to include a sketch of the proof in the Appendix to this paper.

In the proofs of the following two lemmas, we shall ignore problems arising from zero denominators; they can be dealt with by standard tricks as in [5].

<u>Lemma 1</u> : <u>Let</u> ℓ <u>be sufficiently large</u>. <u>Then</u> F_ℓ <u>contains</u> M_ℓ .

<u>Proof</u> : We use an analytic representation of the Weil pairing. Consider the function

$$\Psi_\ell(\underline{z}_1,\underline{z}_2) = \frac{\theta(\ell\underline{z}_1)\ \theta(\underline{z}_2)\ \theta(\underline{z}_1+\ell\underline{z}_2)}{\theta(\ell\underline{z}_2)\ \theta(\underline{z}_1)\ \theta(\underline{z}_2+\ell\underline{z}_1)} .$$

It is readily checked that $\Psi_\ell(\underline{z}_1,\underline{z}_2)$ is an abelian function in each variable separately when the other variable is held fixed. It follows (as in [9] pp.94-96) that $\Psi_\ell(\underline{z}_1,\underline{z}_2)$ is a rational function of $f_1(\underline{z}_1),\dots,f_n(\underline{z}_1)$ and $f_1(\underline{z}_2),\dots,f_n(\underline{z}_2)$. Moreover the coefficients of this rational function can be supposed to lie in F.

Let $E(\underline{z}_1,\underline{z}_2)$ be the Riemann form associated with $\theta(\underline{z})$ (see [7] p.20). We easily verify that

$$(2)\qquad \Psi_\ell(\underline{\omega}_1/\ell,\underline{\omega}_2/\ell) = \exp\{2\pi i E(\underline{\omega}_1,\underline{\omega}_2)/\ell\}$$

for any $\underline{\omega}_1$, $\underline{\omega}_2$ in $\mathcal{L}$. Now $E(\underline{z}_1,\underline{z}_2)$ is integer-valued on the product $\mathcal{L}\times\mathcal{L}$, and we may fix $\underline{\omega}_1$, $\underline{\omega}_2$ such that $E(\underline{\omega}_1,\underline{\omega}_2)\neq 0$. Then (2) implies that $e^{2\pi i/\ell}$ lies in F_ℓ for all ℓ sufficiently large. Hence Lemma 1 is proved.

Next let Γ_ℓ be the Galois group of F_ℓ over F. For all ℓ sufficiently large, there is a standard homomorphism ρ from Γ_ℓ to the multiplicative group of $I/\ell I$. This is defined by the property that for ψ in Γ_ℓ and any σ in I corresponding to $\rho(\psi)$ we have (cf. [7] p. 63 or the Appendix to [1])

$$(3)\qquad (f_i(\underline{\omega}/\ell))^{\psi} = f_i(\underline{\sigma}\,\underline{\omega}/\ell) \quad (1 \leq i \leq n)$$

for any of the generators of F_ℓ. Whenever F_ℓ contains M_ℓ, we write Δ_ℓ for the Galois group of F_ℓ over M_ℓ.

<u>Lemma 2</u> : <u>Let</u> ℓ <u>be sufficiently large</u>. <u>Then for any</u> σ <u>in I corresponding to an element of</u> $\rho(\Delta_\ell)$ <u>we have</u>

$$(4)\qquad \sigma^{\varphi_1}\bar{\sigma}^{\varphi_1} \equiv \sigma^{\varphi_2}\bar{\sigma}^{\varphi_2} \equiv 1 \pmod{\ell} .$$

<u>Proof</u> : Let ψ be an element of Δ_ℓ, and let σ in I correspond to $\rho(\psi)$. Applying ψ to (2) and taking into account the equations (3) , we obtain

$$\exp\{2\pi i E(\underline{\sigma}\,\underline{\omega}_1,\underline{\sigma}\,\underline{\omega}_2)/\ell\} = \exp\{2\pi i E(\underline{\omega}_1,\underline{\omega}_2)/\ell\} .$$

It follows that

$$(5) \qquad E(\underline{\sigma}\underline{\omega}_1, \underline{\sigma}\underline{\omega}_2) \equiv E(\underline{\omega}_1, \underline{\omega}_2) \qquad (\mathrm{mod}\ \ell)$$

for all $\underline{\omega}_1$, $\underline{\omega}_2$ in $\mathcal{L}$.

Next, fix any $\underline{\omega} \neq \underline{0}$ in $\mathcal{L}$. Then according to [7] (Theorem 4, p.48) there exists ζ in K with $\bar{\zeta} = -\zeta$ such that

$$E(\underline{\sigma}_1\underline{\omega}, \underline{\sigma}_2\underline{\omega}) = \mathrm{Tr}(\zeta\sigma_1\bar{\sigma}_2)$$

for all σ_1, σ_2 in I. We deduce that

$$(6) \qquad E(\underline{\sigma}\underline{\sigma}_1\underline{\omega}, \underline{\sigma}\underline{\sigma}_2\underline{\omega}) = \kappa^{\varphi_1}\sigma^{\varphi_1}\bar{\sigma}^{\varphi_1} + \kappa^{\varphi_2}\sigma^{\varphi_2}\bar{\sigma}^{\varphi_2},$$

where

$$\kappa = \kappa(\sigma_1, \sigma_2) = \zeta(\sigma_1\bar{\sigma}_2 - \bar{\sigma}_1\sigma_2).$$

Now the left hand side of (6) is not identically zero in σ_1, σ_2, and hence we may fix σ_1, σ_2 in I such that $\kappa \neq 0$. Put $\underline{\omega}_1 = \underline{\sigma}_1\underline{\omega}$, $\underline{\omega}_2 = \underline{\sigma}_2\underline{\omega}$ in (5); then by (6)

$$(7) \qquad \kappa^{\varphi_1}\sigma^{\varphi_1}\bar{\sigma}^{\varphi_1} + \kappa^{\varphi_2}\sigma^{\varphi_2}\bar{\sigma}^{\varphi_2} \equiv \kappa^{\varphi_1} + \kappa^{\varphi_2} \qquad (\mathrm{mod}\ \ell).$$

But with α_0 as in section 1, we have $\alpha_0^{\varphi_1} = -\alpha_0^{\varphi_2}$ and $\kappa(\sigma_1, \alpha_0\sigma_2) = \alpha_0\kappa(\sigma_1, \sigma_2)$. Hence if we put $\underline{\omega}_1 = \underline{\sigma}_1\underline{\omega}$, $\underline{\omega}_2 = \underline{\alpha}_0\underline{\sigma}_2\underline{\omega}$ in (5), we obtain

$$(8) \qquad \alpha_0^{\varphi_1}(\kappa^{\varphi_1}\sigma^{\varphi_1}\bar{\sigma}^{\varphi_1} - \kappa^{\varphi_2}\sigma^{\varphi_2}\bar{\sigma}^{\varphi_2}) \equiv \alpha_0^{\varphi_1}(\kappa^{\varphi_1} - \kappa^{\varphi_2}) \quad (\mathrm{mod}\ \ell).$$

From (7) and (8) we deduce the congruences (4) of Lemma 2, provided ℓ is sufficiently large.

Lemma 3 : *Let* ℓ *be sufficiently large, and let* δ *in* I *be prime to* ℓ . *Then there are at most* 4 *elements* σ (mod ℓ) *of* I *such that both* σ *and* $\sigma + \delta$ *correspond to elements of* $\rho(\Delta_\ell)$.

Proof : If ℓ is sufficiently large and σ, $\sigma+\delta$ both correspond to elements of $\rho(\Delta_\ell)$ then from Lemma 2 we have

$$(9) \qquad (\sigma+\delta)^{\varphi_1}(\bar{\sigma}+\bar{\delta})^{\varphi_1} \equiv (\sigma+\delta)^{\varphi_2}(\bar{\sigma}+\bar{\delta})^{\varphi_2} \equiv 1 \pmod{\ell}$$

as well as (4). It follows after a simple calculation that $x = \sigma^{\varphi_1}$ satisfies the congruence

$$(10) \qquad \bar{\delta}^{\varphi_1}x^2 + \delta^{\varphi_1}\bar{\delta}^{\varphi_1}x + \delta^{\varphi_1} \equiv 0 \pmod{\ell}.$$

Let $\mathfrak{p}$ be any prime ideal divisor of ℓ in the Galois closure of K. Since δ is prime to ℓ and therefore to $\mathfrak{p}$, (10) shows that there are at most 2 possibilities for $\sigma^{\varphi_1} \pmod{\mathfrak{p}}$. Each of these determines at most one possibility for $\bar{\sigma}^{\varphi_1} \pmod{\mathfrak{p}}$, by (4). A similar argument works for σ^{φ_2} and $\bar{\sigma}^{\varphi_2}$, and we conclude that there are at most 4 possibilities (mod $\mathfrak{p}$) for the quadruple $(\sigma^{\varphi_1}, \bar{\sigma}^{\varphi_1}, \sigma^{\varphi_2}, \bar{\sigma}^{\varphi_2})$. However, we have $\sigma = s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3 + s_4\alpha_4$ for rational integers s_1, s_2, s_3, s_4, and these rational integers can be expressed as fixed linear forms in the conjugates $\sigma^{\varphi_1}, \bar{\sigma}^{\varphi_1}, \sigma^{\varphi_2}, \bar{\sigma}^{\varphi_2}$ of σ. If ℓ is sufficiently large we deduce that there are at most 4 possibilities (mod $\mathfrak{p}$) for the quadruple (s_1, s_2, s_3, s_4), and therefore at most 4 possibilities (mod ℓ). This implies Lemma 3.

The main result of this section can now be proved. It gives a distribution property of the set of $\underline{\sigma} = (\sigma^{\varphi_1}, \sigma^{\varphi_2})$ in $\mathbb{C}^2$ for σ in I corresponding to elements of $\rho(\Delta_\ell)$.

Proposition : *Let ℓ be a sufficiently large prime which does not split in the quadratic field K_0. Then there exist positive constants c, c', c" independent of ℓ such that*

(i) *the field F_ℓ has degree at most $c\ell^3$,*

(ii) *there is a subset D_ℓ of Δ_ℓ, containing at least $c'\ell^2$ elements, such that for any distinct elements σ_1, σ_2 in I corresponding to elements of $\rho(D_\ell)$ we have*

$$(11) \qquad |\underline{\sigma}_1 - \underline{\sigma}_2| > c''\ell^{1/2}.$$

Proof : Let $c_1, c_2 \ldots$ denote positive constants independent of ℓ. We give first the proof of (i), which does not use class field theory or the results of [7]. For $x > 0$ let $I(x)$ be the set of elements δ of I with $0 < |\underline{\delta}| < x$; clearly $I(x)$ contains at most c_1x^4 elements. Now every element δ of $I(\ell^{1/2})$ is prime to

ℓ , because we have

$$|N(\delta)| = |\delta^{\varphi_1}\bar{\delta}^{\varphi_1}\delta^{\varphi_2}\bar{\delta}^{\varphi_2}| = |\delta^{\varphi_1}|^2|\delta^{\varphi_2}|^2 < \ell^2,$$

and the splitting assumption on ℓ implies that every prime ideal factor of ℓ has absolute norm ℓ^2 or ℓ^4. Select λ with $0 < \lambda \leq 1$ arbitrarily for the moment; λ will be specified later during the proof of (ii). Consider the integers $\sigma = s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3 + s_4\alpha_4$ $(0 \leq s_1, s_2, s_3, s_4 < \ell)$ which correspond to elements of $\rho(\Delta_\ell)$; their number is exactly the cardinality of Δ_ℓ. For each δ in $I(\lambda\ell^{1/2})$ delete all the σ such that $\sigma + \delta$ also corresponds to an element of $\rho(\Delta_\ell)$. By Lemma 3, we delete altogether at most $4c_1\lambda^4\ell^2$ integers. The remaining integers (if any) correspond to a subset D_ℓ (possibly empty) of Δ_ℓ, and clearly (11) holds with $c'' = \lambda$ for any distinct σ_1, σ_2 remaining. A simple geometric argument now shows that D_ℓ contains at most $c_2\lambda^{-4}\ell^2$ elements.

Hence Δ_ℓ contains at most $4c_1\lambda^4\ell^2 + c_2\lambda^{-4}\ell^2$ elements, which implies (i), since M_ℓ has degree at most $c_3\ell$.

To verify (ii) we recall that the degree of F_ℓ exceeds $c_4\ell^3$ (see Appendix), and therefore Δ_ℓ contains at least $c_5\ell^2$ elements. Hence, choosing λ above as the largest number with $4c_1\lambda^4 \leq \frac{1}{2}c_5$, we see that D_ℓ is left with at least $\frac{1}{2}c_5\ell^2$ elements. This completes the proof of the Proposition.

The Proposition continues to hold even when ℓ splits in K_0, but then the proof is more elaborate. As we do not need the full result, we omit the details. We end by remarking that the estimate (11) is best possible for any set D_ℓ containing at least $c'\ell^2$ elements.

3. THE AUXILIARY FUNCTION

We return now to the situation in section 1. We suppose α and $\beta = \eta(g,\underline{\omega}) + \alpha(2\pi i)$ are algebraic for $g,\underline{\omega}$ as in the Theorem, and we shall eventually deduce a contradiction. We may assume that the field F of sections 1 and 2 contains α, β and the coefficients in the Taylor expansion of $g(\underline{z})$ about $\underline{z} = \underline{0}$. Recall from [6] that $\partial/\partial z_1$, $\partial/\partial z_2$ map the ring $\mathcal{R} = F[f_1(\underline{z}),\ldots,f_n(\underline{z})]$ into itself. Since $\partial g/\partial z_1$, $\partial g/\partial z_2$ are abelian functions analytic at $\underline{z} = \underline{0}$, there exists h in $\mathcal{R}$, with $h(\underline{0}) \neq 0$, such that $h\,\partial g/\partial z_1$, $h\,\partial g/\partial z_2$ lie in $\mathcal{R}$. Putting $f_{n+1}(\underline{z}) = (h(\underline{z}))^{-1}$, it is easily verified that the ring generated over F by the functions

$$(12) \qquad f_1(\underline{z}),\ldots,f_n(\underline{z}),f_{n+1}(\underline{z}),e^{z_3},g(\underline{z}) + \alpha z_3$$

is mapped into itself by $\partial/\partial z_1$, $\partial/\partial z_2$ and $\partial/\partial z_3$. Also the argument of Lemma 2.1 of [5] shows that for some integer $p \geq 1$ the function $\chi(\underline{z}) = h(\underline{z})(\theta_0(\underline{z}))^p$ is a theta function whose product with any of the functions (12) is entire.

For a large parameter k write

$$L = [k^{4/5}] , \quad S = [k^{1/10}] ,$$

and let c_1, c_2,... denote positive constants independent of k.

<u>Lemma 4</u> : <u>There exists a non-zero polynomial</u> P <u>of degree at most</u> L <u>in each variable</u>, whose <u>coefficients are rational integers of absolute values at most</u> $k^{c_1 k}$, <u>such that for each positive integer</u> $s \leq S$ <u>the function</u>

$$\Phi(\underline{z},z_3) = P(f_1(\underline{z}),\ f_2(z),\ e^{z_3},g(\underline{z}) + \alpha z_3)$$

<u>has a zero of order at least</u> k <u>at</u> $(\underline{z},z_3) = s(\underline{\omega}, 2\pi i)$.

<u>Proof</u> : This is routine. Compare the proof of Lemma 5.1 of [5] , and note that when $(\underline{z},z_3) = s(\underline{\omega}, 2\pi i)$ for an integer s, we have

$$g(\underline{z}) + \alpha z_3 = g(\underline{0}) + s\beta .$$

Next, we need a simple inequality for the absolute height function H defined on the field of algebraic numbers (see [10] , § 1.1 for the definition of the logarithm of H). Let $Q(X_1,\ldots,X_q)$ be a polynomial of degree at most L_i in X_i $(1 \leq i \leq q)$, with rational integer coefficients of absolute values at most U, and for algebraic numbers $\beta_1,\ldots, \beta_q$ put $\gamma = Q(\beta_1,\ldots, \beta_q)$. Then by estimating separately at each valuation we obtain

$$(13) \qquad H(\gamma) \leq U \prod_{i=1}^{q} \{(L_i + 1)(H(\beta_i))^{L_i}\} .$$

<u>Lemma 5</u> : <u>Let</u> ℓ <u>be a sufficiently large prime</u>, <u>and for positive integers</u> $r < \ell$ <u>and</u> s <u>put</u> $t = s + r/\ell$. <u>Then the functions</u> (12) <u>are analytic at</u> $(\underline{z},z_3) = t(\underline{\omega}, 2\pi i)$, <u>and their values at this point lie in</u> F_ℓ <u>and have absolute heights at most</u> $c_2^\ell s$.

Proof : Analyticity follows as on p.247 of [5], since $\chi(\underline{0}) \neq 0$. The corresponding values of all the functions in (12), except possibly the last, lie in F_ℓ by Lemma 1, and their absolute heights are at most c_3 by well-known properties of the Néron-Tate height on A (cf. [2] p.307). We deal with the remaining function as in [5] by noting that $f(\underline{z}) = g(2\underline{z}) - 2g(\underline{z})$ is a rational function of $f_1(\underline{z}),\ldots,f_n(\underline{z})$ with coefficients in F. If $m = 2^{\ell-1} - 1$, the proof of Lemma 3.5 of [5] shows that

$$m(g(t\underline{\omega}) - t\eta) = m(g(r\underline{\omega}/\ell) - r\eta/\ell) = -\sum_{i=0}^{\ell-2} 2^{\ell-2-i}\beta_i,$$

where

$$\beta_i = f(2^i r\underline{\omega}/\ell) \qquad (0 \leq i \leq \ell - 2).$$

Hence $\varepsilon = g(t\underline{\omega}) + \alpha t(2\pi i)$ satisfies

$$m\ell\varepsilon = m(s\ell + r) - \ell\sum_{i=0}^{\ell-2} 2^{\ell-2-i}\beta_i,$$

and so lies in F_ℓ. Again we have $H(\beta_i) \leq c_4^\ell$ $(0 \leq i \leq \ell - 2)$ and so from (13) with $q = \ell$ we deduce $H(m\ell\varepsilon) \leq c_5^\ell s$. This immediately gives the desired estimate for $H(\varepsilon)$, and completes the proof of Lemma 5.

We can now carry out the extrapolation on division values. Let C denote any absolute constant.

Lemma 6 : Let i be an integer with $0 \leq i \leq C$, let $\ell \leq S^{i/8}$ be a sufficiently large prime which does not split in K_0, and for positive integers $r < \ell$ and $s \leq S^{1+(i/4)}$ let $t = s + r/\ell$. Then $\Phi(\underline{z},z_3)$ has a zero of order at least $k/2^i$ at $(\underline{z},z_3) = t(\underline{\omega},2\pi i)$.

Proof : If $i \leq C$ is the first positive integer (if any) for which the lemma is false, there is a differential operator D of minimal order at most $k/2^i$ such that

$$\xi = D\,\Phi(t\underline{\omega}, t(2\pi i)) \neq 0$$

for some t as in the lemma. Since the rational primes which do not split in K_0 have density $\frac{1}{2}$, the number of such primes not exceeding $S^{(i-1)/8}$ is at least $c_6 S^{(i-1)/8}/\log k$. The maximum modulus principle then gives

$$\log|\xi| \leq -c_7 k S^{(i+1)/2}/\log k. \tag{14}$$

But $D\,\Phi(\underline{z},z_3)$ is a polynomial in the functions (12) of total degree at most c_8k. Using (13) and the standard estimates for its coefficients, we deduce from Lemma 5 that

$$\log H(\xi) < c_9 k \log k + c_9 k(\ell + \log s) < c_{10} k s^{1/8}.$$

Again by Lemma 5 we see that ξ lies in F_ℓ, and so by (i) of the Proposition its degree is at most $c_{11}\ell^3$. This leads to

$$\log|\xi| > -c_{12}k\ell^3 s^{1/8} > -c_{12}ks^{1/2}.$$

This contradicts (14) and thereby proves Lemma 6.

At this point let us remark that it is possible to deduce a final contradiction from Lemma 6 by purely analytic methods involving diophantine approximation. This approach does not use the result (ii) of the Proposition. In this way we can obtain a proof of the Theorem independent of class field theory and the results of [7] .

4. COMPLETION OF THE PROOF

We fix a prime ℓ satisfying

$$k^2 < \ell < 2k^2$$

which does not split in K_0. We begin by eliminating $g(\underline{z}) + \alpha z_3$ from the auxiliary function.

Lemma 7 : There is a non-zero polynomial Q of degree at most $M < c_{13}L^2$ in each variable, with coefficients in F, such that for each positive integer $r < \ell$ the function

$$\Psi(\underline{z},z_3) = Q(f_1(\underline{z}),f_2(\underline{z}),e^{z_3})$$

has a zero at $(\underline{z},z_3) = (r/\ell)(\underline{\omega},2\pi i)$.

Proof : The functions $f_1(\underline{z})$, $f_2(\underline{z})$ and $g(\underline{z})$ are algebraically independent (cf. Lemma 2.3 of [5]), and it follows that $\Phi(\underline{z},z_3)$ is not identically zero. An application of Lemma 6 of [4] immediately gives a polynomial Q^* of degree at most $c_{14}L^2$, with coefficients in F, such that the function

$$Q^*(f_1(\underline{z}),\ldots,f_n(\underline{z}),f_{n+1}(\underline{z}),e^{z_3})$$

is not identically zero but vanishes at the points where $\Phi(\underline{z},z_3)$ has a zero of order at least $3L+1$. In particular, by Lemma 6 above with $C = 161$, this function vanishes at the points specified in Lemma 7. There is now no difficulty in constructing the required polynomial Q by the method of Lemma 2.5 of [5], since the ring $F[f_1(\underline{z}),\ldots,f_n(\underline{z})]$ contains $(f_{n+1}(\underline{z}))^{-1}$ and is integral over $F[f_1(\underline{z}),f_2(\underline{z})]$.

The final contradiction is obtained by using the Proposition together with well-known results on polynomials. We need first some preliminary remarks. By the Jacobian condition on $f_1(\underline{z})$ and $f_2(\underline{z})$ at $\underline{z} = \underline{0}$, we may fix a neighbourhood $\mathcal{N}$ of $\underline{z} = \underline{0}$ such that

$$|\underline{f}(\underline{z}_1) - \underline{f}(\underline{z}_2)| > c_{15}|\underline{z}_1 - \underline{z}_2| \tag{15}$$

holds for any $\underline{z}_1$, $\underline{z}_2$ in $\mathcal{N}$, where $\underline{f}(\underline{z}) = (f_1(\underline{z}),f_2(\underline{z}))$. We recall the set D_ℓ of the Proposition, and we let I_ℓ be the set of integers $\sigma = s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3 + s_4\alpha_4$ $(0 \leq s_1,s_2,s_3,s_4 < \ell)$ corresponding to elements of $\rho(D_\ell)$. Let $\mathcal{B}$ be a compact set in $\mathbb{C}^2$ containing all the corresponding points $\underline{\sigma\omega}/\ell$. For any $\mu > 1$ we can cover $\mathcal{B}$ with no more than $c_{16}\,\mu^{20}$ small balls of radius μ^{-5}. Since I_ℓ contains at least $c_{17}\,\ell^2$ elements, there exists a subset J_ℓ of I_ℓ, containing at least $c_{18}\,\mu^{-20}\,\ell^2$ elements σ, such that the corresponding points $\underline{\sigma\omega}/\ell$ all lie in the same ball, say $\mathcal{B}_0$. Let $\underline{z}_0$ be the centre of $\mathcal{B}_0$. A less direct application of the Box Principle gives an integer r with $1 \leq r \leq \mu^4$ such that

$$|r\underline{z}_0 - \underline{\omega}_0| < c_{19}\,\mu^{-1}$$

for some period $\underline{\omega}_0$ of $\mathcal{L}$. It follows that for any $\underline{z}$ in $\mathcal{B}_0$ we have

$$|r\underline{z} - \underline{\omega}_0| \leq r|\underline{z} - \underline{z}_0| + c_{19}\mu^{-1} < c_{20}\,\mu^{-1}. \tag{16}$$

We now fix $\mu < c_{21}$ so large that (16) implies that $r\underline{z} - \underline{\omega}_0$ lies in $\mathcal{N}$ for all $\underline{z}$ in $\mathcal{B}_0$. Hence by (15) and (11), we conclude that

$$|\underline{f}(r\underline{\sigma}_1\underline{\omega}/\ell) - \underline{f}(r\,\underline{\sigma}_2\underline{\omega}/\ell)| > c_{22}|\underline{\sigma}_1 - \underline{\sigma}_2|/\ell > c_{23}\ell^{-1/2} \tag{17}$$

for any distinct σ_1, σ_2 in J_ℓ .

We now return to Lemma 7. Since $M < c_{13}L^2$, $r < c_{24}$ and $\ell > k^2$, ordinary cyclotomy shows that the polynomial

$$R(X_1, X_2) = Q(X_1, X_2, e^{2\pi ir/\ell})$$

is not identically zero. We have also

$$R(f_1(r\underline{\omega}/\ell), f_2(r\underline{\omega}/\ell)) = 0. \tag{18}$$

Let σ be an element of J_ℓ , and apply the corresponding automorphism ψ of Δ_ℓ to (18). Since ψ fixes $M_\ell = F(e^{2\pi i/\ell})$, we find using (3) that

$$R(f_1(r\underline{\sigma}\underline{\omega})/\ell),\ f_2(r\underline{\sigma}\underline{\omega}/\ell)) = 0 \quad .$$

Because J_ℓ contains at least $c_{25}\ell^2$ elements, it follows from (17) and the usual estimates for zeroes of polynomials (e.g. Lemma 8 of [6]) that R is identically zero. This contradiction completes the proof of the Theorem.

APPENDIX

Lower bounds for degrees of division fields.

We prove here the main fact used in section 3, namely that the field F_ℓ has degree at least $c\ell^3$ for some $c > 0$ independent of ℓ. The proof is based on an argument shown to me by Shimura during the conference, and I am grateful for his permission to include it in this paper.

Since the abelian variety A is simple, the CM-type dual to $(K;\varphi_1, \varphi_2)$ has the same form $(K^*;\psi_1, \psi_2)$ (see [7] section 8, and especially pp. 73, 74). Fix $\underline{\omega} \neq \underline{0}$ in $\mathcal{L}$, and let $\underline{t} = \underline{\omega}/\ell$. If ℓ is sufficiently large then $\theta_0(\underline{t}) \neq 0$ and $\underline{t}$ is a proper $\mathfrak{b}$-section point of A in the sense of [7] (p.63), where $\mathfrak{b}$ is the principal ideal of K generated by ℓ . We now appeal to the Main Theorem 2 of [7] (p.135, but see also p.118 ; this is where we need our hypothesis on the endomorphism ring of A). Using the basic properties of Kummer varieties and fields of moduli ([7] Proposition 16, p.30, and Theorem 2, p.28), it is not hard to see that our field F_ℓ contains the class field K_ℓ over K^* specified in Main Theorem 2. This corresponds to the ideal group H_ℓ of K^* defined (mod ℓ) as follows. The ideal $\mathfrak{a}$ of K^* prime to ℓ is in H_ℓ if and only if the ideal $\mathfrak{a}^{\psi_1}\mathfrak{a}^{\psi_2}$ of K is the principal ideal generated by an element μ of K such that $\mu\bar{\mu}$ is the absolute norm of $\mathfrak{a}$ and $\mu \equiv 1 \pmod{\ell}$.

Thus if G_ℓ is the group of ideals of K^* prime to ℓ, the Galois group of K_ℓ over K^* is isomorphic to G_ℓ / H_ℓ, and we proceed to show that the latter quotient has order at least $c' \ell^3$ for some $c' > 0$ independent of ℓ.

To each λ in I prime to ℓ we associate the principal ideal of K^* generated by $\lambda^{\varphi_1}\lambda^{\varphi_2}$. This induces a homomorphism Φ from the multiplicative group of $I/\ell I$ to G_ℓ / H_ℓ. It suffices to prove that the kernel $\ker(\Phi)$ of Φ has order at most $c''\ell$ for some c'' independent of ℓ. However, let λ in I prime to ℓ correspond to an element of this kernel. Then after an easy calculation (see [7] pp. 73,74) we find that the resulting element μ of K must be of the form $\varepsilon\lambda N(\lambda)/\bar{\lambda}$, where ε is a root of unity in K. Now there exists a positive integer $m \leq 12$ independent of ε such that $\varepsilon^m = 1$, and we deduce that $\lambda^m(N(\lambda))^m \equiv \bar{\lambda}^m \pmod{\ell}$. This, together with its complex conjugate, implies that

$$(N(\lambda))^{2m} = (\lambda^{\varphi_1}\bar{\lambda}^{\varphi_1}\lambda^{\varphi_2}\bar{\lambda}^{\varphi_2})^{2m} \equiv 1 \pmod{\ell}, \tag{19}$$

and also $\lambda^{2m} \equiv \bar{\lambda}^{2m} \pmod{\ell}$. Applying φ_1, φ_2 to the latter congruence, we obtain

$$(\lambda^{\varphi_1})^{2m} \equiv (\bar{\lambda}^{\varphi_1})^{2m}, \quad (\lambda^{\varphi_2})^{2m} \equiv (\bar{\lambda}^{\varphi_2})^{2m} \pmod{\ell}. \tag{20}$$

Fix any integer r with $0 \leq r < \ell$, and let N_r be the number of integers $\lambda \pmod{\ell}$ in I, prime to ℓ, such that (19) and (20) hold as well as

$$\mathrm{Tr}(\lambda^{4m}) = (\lambda^{\varphi_1})^{4m} + (\bar{\lambda}^{\varphi_1})^{4m} + (\lambda^{\varphi_2})^{4m} + (\bar{\lambda}^{\varphi_2})^{4m} \equiv r \pmod{\ell}.$$

For any such λ, the number $x = (\lambda^{\varphi_1})^{4m}$ satisfies

$$2x^2 - rx + 2 \equiv 0 \pmod{\ell}.$$

A simple counting argument, as in the proof of Lemma 3, now shows that $N_r \leq 2(4m)^4$ for ℓ sufficiently large. It follows that in this case $\ker(\Phi)$ contains at most $2(4m)^4\ell$ elements, and this leads to the desired lower bounds for the degree of F_ℓ.

REFERENCES

[1] M. Anderson, Linear forms in algebraic points of an elliptic function, Transcendence theory : advances and applications (Eds. A. Baker and D. W. Masser), Academic Press, London (1977).

[2] S. Lang, Diophantine approximation on abelian varieties with complex multiplication, Advances in Math. 17 (1975), 281-336.

[3] S. Lefschetz, Algebraic geometry, Oxford University Press, London 1953.

[4] D. W. Masser, Some vector spaces associated with two elliptic functions, Transcendence theory : advances and applications (Eds. A. Baker and D. W. Masser), Academic Press, London 1977.

[5] D. W. Masser, The transcendence of certain quasi-periods associated with abelian functions in two variables, Compositio Math. 35 (1977), 239-258.

[6] D. W. Masser, Diophantine approximation and lattices with complex multiplication, Inventiones Math. 45 (1978), 61-82.

[7] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan Vol. 6, Tokyo 1961.

[8] G. Shimura, Automorphic forms and the periods of abelian varieties, J. Math. Soc. Japan 31 (1979), 561-592.

[9] C. L. Siegel, Topics in complex function theory, Vol. III, Wiley-Interscience, New York 1963.

[10] M. Waldschmidt, Nombres transcendants et groupes algébriques, Astérisque 69-70, 1979.

Department of Mathematics
University of Nottingham
University Park
Nottingham NG7 2RD
(United Kingdom)