MÉMOIRES DE LA S. M. F.

W. DALE BROWNAWELL

On the orders of zero of certain functions

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 5-20

<http://www.numdam.org/item?id=MSMF_1980_2_2__5_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 5-20

ON THE ORDERS OF ZERO OF CERTAIN FUNCTIONS

by

W. Dale BROWNAWELL[♦]

I. INTRODUCTION

This is a report on joint work with D. W. Masser into the possible order of vanishing of a certain class of analytic functions. A complete exposition of our most general result and its relation to the previous work of Ju. Nesterenko [4] is given in [1] . That paper was written expressly for the use of fellow practitioners of transcendence theory.

For this conference it seemed appropriate to present a variant of the proof of the main theorem of [1] , this time assuming familiarity with commutative algebra from the outset. The major change is the use here of the Hilbert characteristic function $H_a(\mathfrak{a},t)$ for inhomogeneous ideals $\mathfrak{a}$. In this way we avoid the technicalities involved in keeping track of the order of vanishing while homogenizing and dehomogenizing ideals. (These technicalities seem indispensable however for handling denominators in some of Masser's most recent work). Since we have not found a reference for the properties of $H_a(\mathfrak{a},t)$ in the literature (see [2,p. 157] however), we discuss them in a short appendix following the body of the proof.

We are concerned here with solutions of a fixed system of differential equations

[♦] Research supported in part by the National Science Foundation.

$$(1) \qquad f_i' = F_i(f_1,\dots,f_n) \qquad (1 < i < n)$$

where $F_1,\dots,F_n$ are non-zero polynomials of total degree at most d. For a given set of initial values $\Theta = (\theta_1,\dots,\theta_n)$, we denote by $\bar{f}(z;\Theta)$ the corresponding solution of (1) analytic at the origin, i.e. the coordinates $f_1(z;\Theta),\dots,f_n(z;\Theta)$ satisfy (1) and $\bar{f}(0,\Theta) = \Theta$. In this paper we will deal with $M+1$ fixed such initial conditions given by $\Theta_0, \Theta_1,\dots, \Theta_M$.

Let $\mathfrak{a}$ be an ideal of $R = \mathbb{C}[X_1,\dots,X_n]$. For $0 < m < M$ we define

$$\mathrm{ord}_m\, \mathfrak{a} = \min_{\substack{P \in \mathfrak{a} \\ P \neq 0}} \mathrm{ord}\, P(\bar{f}(z;\Theta_m)),$$

where ord on the right hand side denotes the order of zero at the origin with the usual proviso that ord $0 = \infty$. Say $\mathfrak{a}$ is generated by $P_1,\dots,P_s$. Then clearly

$$\mathrm{ord}_m\, \mathfrak{a} = \min_i \mathrm{ord}\, P_i(\bar{f}(z;\Theta_m)).$$

If $\mathfrak{a}$ has rank r (we avoid the term "height" because of other associations in transcendence theory), we can suppose that the indices are chosen in such a way that $P_1,\dots,P_r$ have total degrees at most $D_1 > \dots > D_r$, respectively, whereas $P_{r+1},\dots,P_s$ have total degrees at most D_r. Let $T = D_1 \dots D_r$, and recall that $d < \max_i \deg F_i$. Then we can state our main result.

__Theorem__ : __Assume that__ $\mathrm{ord}_m\, \mathfrak{a}$ __is finite for__ $0 < m < M$. __Then if__ $r < n$ __and__ $d > 1$, __we have__

$$\sum_{m=0}^{M} \mathrm{ord}_m\, \mathfrak{a} < (dT)^{2^{n-r}} + M(dT)^{2^{n-r-1}},$$

__while if__ $r < n$ __and__ $d = 1$, __we have__

$$\sum_{m=0}^{M} \mathrm{ord}_m\, \mathfrak{a} < (n-r+1)D_1^{n-r}T + (n-r)MTD_1^{n-r-1}.$$

__Finally if__ $r = n$, __then__

$$\sum_{m=0}^{M} \mathrm{ord}_m\, \mathfrak{a} < T.$$

II. UNMIXING

Because we can estimate the degree of an ideal of the principal class (rank = minimal number of generators) through Proposition 4A, we would be very happy if r = s. Since that is not always the case, we show that for our purposes, it is always possible to replace $\mathfrak{A}$ by an ideal $\mathfrak{A}_r$ of rank r and generated by r polynomials of degrees at most $D_1,\dots,D_r$, respectively, such that

$$\mathrm{ord}_m \mathfrak{A}_r = \mathrm{ord}_m \mathfrak{A} \qquad (0 < m < M).$$

For that the following general remark is useful.

Lemma 1 : Let $P_1,\dots,P_s$ be polynomials and let $\vartheta_1,\dots,\vartheta_k$ be ideals such that for each $1 < \kappa \leq k$, not all of $P_1,\dots,P_s$ lie in ϑ_κ. Then for some integer, $1 < \lambda < ks$,

$$P_1 + \lambda P_2 + \dots + \lambda^{s-1} P_s \notin \bigcup_{\kappa=1}^{k} \vartheta_k .$$

Proof : If each of the $Q_\lambda = P_1 + \lambda P_2 + \dots + \lambda^{s-1} P_s$ $(1 < \lambda < ks)$ lies in some ϑ, then by the Box Principle, at least s of the Q_λ lie in the same ϑ. Inverting the corresponding Vandermonde determinant shows then that $P_1,\dots,P_s$ all lie in that same ϑ as well. This contradiction establishes the lemma.

For a vector $\Theta = (\theta_1,\dots,\theta_n)$ of $\mathbb{C}^n$ we denote by $\mathfrak{M}(\Theta)$ the corresponding maximal ideal $(x_1 - \theta_1,\dots, x_n - \theta_n)$. For brevity we write $\mathfrak{M}_0,\dots,\mathfrak{M}_M$ instead of $\mathfrak{M}(\Theta_0),\dots,\mathfrak{M}(\Theta_M)$, respectively. For $0 < m < M$ we write $\mathfrak{A}^{(m)}$ for the contracted extension

$$\mathfrak{A}^{(m)} = \mathfrak{A}_m \cap R ,$$

where $\mathfrak{A}_m$ denotes the extension of $\mathfrak{A}$ to the localization of $R = \mathbb{C}[x_1,\dots,x_n]$ at $\mathfrak{M}_m$. Further we write $\overset{*}{\mathfrak{A}}$ for the contracted extension with respect to the multiplicative set $S = R \setminus \bigcup_{m=0}^{M} \mathfrak{M}_m$, i.e. $\overset{*}{\mathfrak{A}} = (\mathfrak{A} \otimes_R R_S) \cap R$. We see that $\overset{*}{\mathfrak{A}}$ is also obtained by deleting from a primary decomposition of $\mathfrak{A}$ components not lying in any $\mathfrak{M}_m$ $(0 < m < M)$, just as $\mathfrak{A}^{(m)}$ is obtained on deleting components not in $\mathfrak{M}_m$. Therefore

$$\overset{*}{\mathfrak{A}} = \bigcap_{m=0}^{M} \mathfrak{A}^{(m)} . \tag{2}$$

Since every element of $\mathfrak{a}^{(m)}$ is the quotient of an element of $\mathfrak{a}$ by an element outside $\mathfrak{M}_m$, we see that $\mathrm{ord}_m\,\mathfrak{a}^{(m)} = \mathrm{ord}_m\,\mathfrak{a}$. Therefore from $\mathfrak{a} \subseteq \mathfrak{a}^* \subseteq \mathfrak{a}^{(m)}$ we deduce that

$$\text{(3)} \qquad \mathrm{ord}_m\,\mathfrak{a} = \mathrm{ord}_m\,\mathfrak{a}^* = \mathrm{ord}_m\,\mathfrak{a}^{(m)} \qquad (0 \leq m \leq M)$$

<u>Proposition 2</u> : <u>If in addition to the hypotheses of the Main Theorem we have</u>

$$0 < \mathrm{ord}_m\,\mathfrak{a} \qquad (0 \leq m \leq M)\ ,$$

<u>then there are polynomials</u> $Q_1,\dots,Q_r$ <u>in</u> $\mathfrak{a}$ <u>with</u> $\deg Q_1 \leq D_1,\dots,\deg Q_r \leq D_r$ <u>such that the ideal</u> $\mathfrak{a}_r = (Q_1,\dots,Q_r)$ <u>satisfies</u>

$$\mathrm{rank}\ \mathfrak{a}_r = r\ ,$$

$$\mathrm{ord}_m\,\mathfrak{a}_r = \mathrm{ord}_m\,\mathfrak{a} \qquad (0 \leq m \leq M),$$

<u>and</u>

$$\deg \mathfrak{a}_r^* \leq D_1\dots D_r = T\ .$$

<u>Proof</u> : Since $\mathrm{ord}_m\,\mathfrak{a}$ is assumed to be finite for each m, the polynomials P such that $\mathrm{ord}_m P > \mathrm{ord}_m\,\mathfrak{a}$ form an ideal which we denote $\mathfrak{b}_m$. By Lemma 1 we can select $\lambda \in \mathbb{Z}$ such that

$$Q_1 = P_1 + \lambda P_2 + \dots + \lambda^{s-1} P_s \notin \bigcup_{m=0}^{M} \mathfrak{b}_m .$$

Set $\mathfrak{a}_1 = (Q_1)$. Then $\mathrm{rank}\ \mathfrak{a}_1 = 1$ and $\mathrm{ord}_m\,\mathfrak{a}_1 = \mathrm{ord}_m\,\mathfrak{a}$, $0 \leq m \leq M$. Now $\mathfrak{a}_1^*$ is principal with generator obtained from Q_1 by deleting all factors not in any $\mathfrak{M}_m$, $0 \leq m \leq M$. Since $\mathrm{ord}_m\,\mathfrak{a}_1^* = \mathrm{ord}_m\,\mathfrak{a}_1 > 0$, Q_1 is not constant and $\mathrm{rank}\ \mathfrak{a}_1^* = 1$. We deduce from Proposition 4A of the appendix that

$$\deg \mathfrak{a}_1^* \leq D_1\ ,$$

which is what was claimed for $r = 1$.

For $r > 1$ we choose polynomials $Q_2, \ldots, Q_r$ inductively of the form

$$(4) \qquad Q_i = P_i + \lambda_i P_{i+1} + \ldots + \lambda_i^{s-i} P_s$$

such that the ideals $\mathfrak{a}_i = (Q_1, \ldots, Q_i)$ satisfy

$$\operatorname{rank} \mathfrak{a}_i = i, \ \deg \mathfrak{a}_i^* \leq D_1 \ldots D_i \ .$$

Moreover the form of selection given in (4) guarantees that for $1 \leq i \leq r$

$$\operatorname{ord}_m \mathfrak{a}_i = \operatorname{ord}_m \mathfrak{a} \qquad\qquad (0 \leq m \leq M)$$

The selection has already been made for $i = 1$, and now we show how to find Q_{i+1} with the desired properties once $\mathfrak{a}_i$ has been obtained $(i < r)$.

Fix a prime component $\mathfrak{p}$ of $\mathfrak{a}_i$ of rank i (necessarily so by the Cohen-Macauley Theorem [5-II ,p.310]). If $P_{i+1}, \ldots, P_s$ all lay in $\mathfrak{p}$, Then we see inductively from (4) that so do P_i, $P_{i-1}, \ldots, P_1$. Thus $\mathfrak{a}$ would be contained in $\mathfrak{p}$ and rank $\mathfrak{a} \leq i$, contrary to our assumption that rank $\mathfrak{a} = r$. Thus at least one of $P_{i+1}, \ldots, P_s$ does not lie in $\mathfrak{p}$. So by Lemma 1, there is a Q_{i+1} of the form (4) not in any prime component of $\mathfrak{a}_i$, i.e. $\mathfrak{a}_i : Q_{i+1} = \mathfrak{a}_i$. Therefore by Proposition 4A of the appendix, for $\mathfrak{a}_{i+1} = (\mathfrak{a}_i, Q_{i+1})$ we have rank $\mathfrak{a}_{i+1} = i+1$ and $\deg \mathfrak{a}_{i+1} \leq (\deg \mathfrak{a}_i) D_{i+1}$, which establishes Proposition 2.

III. THE CASE $n = r$.

To deal with this case we require a fundamental result concerning exponents of ideals.

Lemma 3 : If $\mathfrak{q}$ is a primary ideal of length ℓ and exponent e, then $e \leq \ell$.

Proof : Say that $\mathfrak{q}$ is $\mathfrak{p}$-primary. Then $\mathfrak{p}^e \subseteq \mathfrak{q}$, and e is the least positive power of $\mathfrak{p}$ lying in $\mathfrak{q}$. If $e = 1$, then $\mathfrak{p} = \mathfrak{q}$ and there is nothing to show. If $e \geq 2$, the ideals $\mathfrak{q}_i = \mathfrak{q} : \mathfrak{p}^i$ $(0 \leq i < e)$ are $\mathfrak{p}$ -primary [5-I, p.154] . Since $\mathfrak{p}^{e-1}\mathfrak{p} = \mathfrak{p}^e \subseteq \mathfrak{q}$, $\mathfrak{p} \subset \mathfrak{q}_{e-1}$, and so $\mathfrak{p} = \mathfrak{q}_{e-1}$. Thus we obtain e primary ideals

$$\mathfrak{q} = \mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subsetneq \cdots \subseteq \mathfrak{q}_{e-1} = \mathfrak{p}$$

If we can show that these inclusions are strict, then the lemma will follow. But $\mathfrak{p}\mathfrak{q}_{k+1} \subseteq \mathfrak{q}_k$ $(0 \leq k < e-1)$. So if some $\mathfrak{q}_k = \mathfrak{q}_{k+1}$, then $\mathfrak{p}\mathfrak{q}_{k+2} \subseteq \mathfrak{q}_{k+1} = \mathfrak{q}_k$. Therefore $\mathfrak{p}^{k+1}\mathfrak{q}_{k+2} \subseteq \mathfrak{p}^k\mathfrak{q}_k \subseteq \mathfrak{q}$ and $\mathfrak{q}_{k+2} \subseteq \mathfrak{q}_{k+1}$. Consequently $\mathfrak{q}_k = \mathfrak{q}_{k+1} = \mathfrak{q}_{k+2}$. Repeating the argument shows that

$$\mathfrak{q}_k = \mathfrak{q}_{k+1} = \dots = \mathfrak{q}_{e-1} .$$

Thus $\mathfrak{p} = \mathfrak{q} : \mathfrak{p}^k$ and $\mathfrak{p}^{k+1} \subseteq \mathfrak{q}$. By the definition of e, $e \leq k+1$. But $k+1 \leq e-1$ by assumption. This contradiction shows that the inclusions are strict and establishes the lemma.

Proposition 4 : Let $\mathfrak{q}$ be primary of rank n such that $\mathrm{ord}_m \mathfrak{q}$ is positive but finite for some $0 \leq m \leq M$. Then $\mathfrak{M}_m$ is the associated prime ideal of $\mathfrak{q}$ and

$$\mathrm{ord}_m \mathfrak{q} \leq \deg \mathfrak{q}.$$

Proof : Since $\mathrm{ord}_m \mathfrak{q} > 0$, we have $\mathfrak{q} \subset \mathfrak{M}_m$. Because rank $\mathfrak{q} = n$, $\mathfrak{M}_m$ is the associated prime. Let e be the exponent of $\mathfrak{q}$. Then

$$\mathfrak{M}_m^e \subseteq \mathfrak{q} \subseteq \mathfrak{M}_m.$$

Since for any ideals $\mathfrak{k}, \mathfrak{L}$

$$\mathrm{ord}_m(\mathfrak{k} \cap \mathfrak{L}) \leq \mathrm{ord}_m(\mathfrak{k}\mathfrak{L}) = \mathrm{ord}_m \mathfrak{k} + \mathrm{ord}_m \mathfrak{L},$$

we see that

$$\mathrm{ord}_m \mathfrak{q} \leq e \,\mathrm{ord}_m \mathfrak{M}_m.$$

From Proposition 2A of the appendix and Lemma 4 we see that

$$e \leq \mathrm{length}\, \mathfrak{q} \leq \deg \mathfrak{q}.$$

If $\Theta_m = (\theta_1, \dots, \theta_n)$, then $\mathrm{ord}_m \mathfrak{M}_m = \min_i \mathrm{ord}_m(f_i(z;\Theta_m) - \theta_i)$, and so if $\mathrm{ord}_m \mathfrak{M}_m > 1$, then each $f_i'(z;\Theta_m)$ vanishes at the origin. Now differentiation of (1) leads to the relations

$$f_i''(z;\,\Theta_m) = \sum_{j=1}^{n} \left.\frac{\partial F_i}{\partial x_j}\right|_{\bar{f}(z;\,\Theta_m)} f_j'(\,z\,;\,\Theta_m) \qquad (1\leq i\leq n).$$

Thus

$$\operatorname{ord}_{z=o} f_i''(z;\,\Theta_m) \geq \min_j \operatorname{ord}_{z=o} f_j'(z;\,\Theta_m) > 0 \qquad (1\leq i\leq n).$$

This implies that $\operatorname{ord}_{z=o} f_i'(z;\,\Theta_m) = \infty$, $1 < i < n$. Then $\operatorname{ord}_m \mathfrak{M}_m = \infty$, a contradiction which completes the proof of the proposition.

Proof of the case n = r.

We may clearly assume that $\operatorname{ord}_m \mathfrak{a} > 0$ $(0\leq m\leq M)$ simply by renumbering and taking M smaller if necessary. For if the analogous bound holds on the sum of the remaining $\operatorname{ord}_m \mathfrak{a}$, then the desired bound will hold on the full sum. We apply Proposition 2 to $\mathfrak{a}$ to obtain $\mathfrak{a}_n$. If $\mathfrak{a}_n^* = \mathfrak{q}_o \cap\dots\cap \mathfrak{q}_N$ is the primary decomposition of $\mathfrak{a}_n^*$, then by the first half of Proposition 4, N = M, and we may take $\mathfrak{q}_m$ to be $\mathfrak{p}_m$-primary $(0\leq m\leq M)$. By the second half of Propositions 3A and 4A of the appendix and by Proposition 4,

$$\begin{aligned} T \geq \deg \mathfrak{a}_n^* &= \sum_{m=o}^{M} \deg \mathfrak{q}_m \\ &\geq \sum_{m=o}^{M} \operatorname{ord}_m \mathfrak{q}_m = \sum_{m=o}^{M} \operatorname{ord}_m \mathfrak{a}, \end{aligned}$$

since $\operatorname{ord}_m \mathfrak{a} = \operatorname{ord}_m \mathfrak{a}_n = \operatorname{ord}_m \mathfrak{a}_n^{(m)} = \operatorname{ord}_m \mathfrak{q}_m$ $(0\leq m\leq M)$. This proves the assertion of the theorem for r = n.

IV. INCREASING THE LOCAL RANK

In this section we develop a procedure which allows us to cope with ideals of rank less than n. We inductively produce polynomials $Q_{r+1},\dots,Q_n$ of predictably bounded degrees $D_{r+1},\dots,D_n$, respectively, through differentiation of the generators of $\mathfrak{a}_r$ such that for $r\leq i\leq n$ the ideals

(7) $$\mathcal{L}_i = (\,\mathfrak{a}_r, Q_{r+1},\dots,Q_i)$$

satisfy

(8) $$\operatorname{rank} \mathcal{B}_i^{(m)} = i \qquad (0 \le m \le M) ,$$

(9) $$\deg \mathcal{B}_i^* \le D_1 \ldots D_i$$

and

(10) $$\operatorname{ord}_m \mathcal{A} - W_{i-r-1} \le \operatorname{ord}_m \mathcal{B}_i \ne \infty \qquad (0 \le m \le M)$$

where

$$W_k = \begin{cases} \sum\limits_{j=o}^{k} d^{2^j-1} T^{2^j}, & \text{if } d > 1 \\ T \sum\limits_{j=o}^{k} D_1^j , & \text{if } d = 1. \end{cases}$$

(Recall that d is our upper bound on the degree of the polynomials $F_1, \ldots, F_n$ in (1) and D_1 bounds the degree of all the generators of $\mathcal{A}$). As we shall see, W_{i-r-1} is a bound on the number of derivatives we may have to take to obtain $Q_{r+1}, \ldots, Q_i$. Because of its importance for the Main Theorem, we state the result for i = n as a proposition. Set

$$D_i = \begin{cases} (dT)^{2^{i-r-1}} , & \text{if } d > 1 \\ D_1, & \text{if } d = 1 \end{cases}$$

<u>Proposition 5</u> : <u>Given</u> $\mathcal{A}_r$ <u>of Proposition</u> 2 <u>with</u>

$$W_{n-r-1} < \operatorname{ord}_m \mathcal{A}_r \ne \infty \qquad (0 \le m \le M),$$

<u>there are then polynomials</u> $Q_{r+1}, \ldots, Q_n$ <u>with</u> $\deg Q_i \le D_i$ $(r < i \le n)$ <u>such that the following holds for</u> $\mathcal{B}_n = (\mathcal{A}_r, Q_{r+1}, \ldots, Q_n)$:

$$\operatorname{rank} \mathcal{B}_n^{(m)} = n, \ \operatorname{ord}_m \mathcal{A}_r - W_{n-r-1} \le \operatorname{ord}_m \mathcal{B}_n \qquad (0 \le m \le M)$$

and

$$\deg \mathcal{B}_n^* \le D_1 \ldots D_n .$$

Proof : As mentioned above, the construction of the $\mathfrak{b}_{r+1},\ldots,\mathfrak{b}_n$ with the properties (8), (9), (10) is inductive. If we set $W_{-1} = 0$, we may consider $\mathfrak{b}_r = \mathfrak{a}_r$ to start it off. For the inductive step assume that (8), (9), (10) hold for some $\mathfrak{b}_i$ of the form (7), $r \leq i < n$. Consider the derivation

$$\Delta = \sum_{j=1}^{n} F_j \frac{\partial}{\partial x_j}$$

defined on $R = \mathbb{C}[x_1,\ldots,x_n]$. Clearly if $P \in R$ has total degree G, then ΔP has total degree at most $G + d - 1$. Also if $\bar{f} = (f_1,\ldots,f_n)$ is an analytic solution of (1) then for any polynomial $P \in R$,

$$\Delta P(\bar{f}) = \frac{d}{dz} P(\bar{f}).$$

So if $\text{ord}_m P \geq 1$, then $\text{ord}_m \Delta P = \text{ord}_m P - 1$ $(C \leq m \leq M)$. Since the ideals $\mathfrak{b}_i^{(m)}$ have rank i and $\mathfrak{b}_i$ is generated by i elements, $\mathfrak{b}_i^{(m)}$ is unmixed by the Cohen-Macauley Theorem [5-II, p.310] . Therefore in particular all primary components of $\mathfrak{b}_i^*$ have rank i. For the next few paragraphs we consider one fixed such component $\mathfrak{q}$ and its associated prime $\mathfrak{p}$.

From Lemma 3, Propositions 2A and 3A of the appendix, and our induction assumption, we deduce that

$$e \leq \deg \mathfrak{a}_i^* \leq D_1 \ldots D_i \tag{11}$$

for the exponent e of $\mathfrak{q}$. We claim that

$$\Delta^e \mathfrak{b}_i^* \nsubseteq \mathfrak{p}. \tag{12}$$

Since $\mathfrak{b}_i^* \subseteq \mathfrak{p} \subseteq \mathfrak{m}_m$ for some $0 \leq m \leq M$, $\text{ord}_m \mathfrak{p}$ is positive but bounded by $\text{ord}_m \mathfrak{b}_i^*$. Choose a polynomial $P \in \mathfrak{p}$ with $\text{ord}_m P = \text{ord}_m \mathfrak{p}$. Since

$$\text{ord}_m \Delta P = \text{ord}_m P - 1 < \text{ord}_m \mathfrak{p},$$

ΔP does not lie in $\mathfrak{p}$. Let Q be a polynomial lying in every primary component $\mathfrak{q}' \neq \mathfrak{q}$ of $\mathfrak{b}_i^*$ and not lying in $\mathfrak{p}$ – for example the product of elements from each $\mathfrak{q}' \setminus \mathfrak{p}$. From the definition of exponent we know that P^e lies in $\mathfrak{q}$. So $P^e Q$ lies in $\mathfrak{b}_i^*$. Moreover since P lies in $\mathfrak{p}$,

$$\Delta^e (P^e Q) \equiv e!(\Delta P)^e Q \qquad (\text{mod } \mathfrak{p}).$$

Since neither Q nor ΔP is in $\mathfrak{p}$, this establishes (12), a crucial step in our proof.

Now let t be the least positive integer such that $\Delta^t \mathcal{B}_i^* \not\subseteq \mathfrak{p}$. From (11) and (12) we see that

$$t \leq e \leq D_1 \ldots D_i .$$

We claim that

$$\Delta^t \mathcal{B}_i \not\subseteq \mathfrak{p}. \tag{13}$$

For there is a B in $\mathcal{B}_i^*$ such that $\Delta^t B$ is not in $\mathfrak{p}$. From the definition of $\mathcal{B}_i^*$, there is an A outside $\bigcup_{m=o}^{M} \mathcal{M}_m$ such that C = AB lies in $\mathcal{B}_i$. From the minimality of t we see that each $\Delta^\tau B$ lies in $\mathfrak{p}$ for $0 \leq \tau < t$ and thus that

$$\Delta^t C \equiv A \, \Delta^t B \qquad (\text{mod } \mathfrak{p}).$$

Since A is not in any $\mathcal{M}_m$, it is not in $\mathfrak{p}$ either, for, as we noted above, $\mathfrak{p} \subseteq \mathcal{M}_m$ for some $0 \leq m \leq M$. We deduce that $\Delta^t C$ is not in $\mathfrak{p}$, which verifies (13).

Since for $0 \leq \tau \leq t$

$$\Delta^\tau \mathcal{B}_i \subseteq \Delta^\tau \mathcal{B}_i^* \subseteq \mathfrak{p} ,$$

the integer t is also minimal with respect to the property (13). Write

$$C = A_1 Q_1 + \ldots + A_i Q_i$$

with $A_1, \ldots, A_i$ in R. Then by the minimality of t,

$$\Delta^t C \equiv A_1 \, \Delta^t Q_1 + \ldots + A_i \, \Delta^t Q_i \qquad (\text{mod } \mathfrak{p}).$$

Hence $\Delta^t Q_j$ is not in $\mathfrak{p}$ for some $1 \leq j \leq i$. By (11), since $t \leq e$, $\Delta^t Q_j$ has total degree at most

$$\max(D_1, D_i) + (d-1) D_1 \ldots D_i \leq D_{i+1} .$$

Moreover

$$\begin{aligned}\operatorname{ord}_m \Delta^t Q_j &\geqslant \operatorname{ord}_m \mathcal{B}_i - t\\ &\geqslant \operatorname{ord}_m \mathfrak{A}_r - W_{i-r-1} - t\\ &\geqslant \operatorname{ord}_m \mathfrak{A}_r - W_{i-r} .\end{aligned}$$

When we carry out this construction for each of the prime components $\mathfrak{p}_1,\dots,\mathfrak{p}_k$ of each $\mathcal{B}_i^{(m)}$ $(0 \leqslant m \leqslant M)$, we obtain polynomials $L_1,\dots,L_k$ of degrees at most D_{i+1} such that

$$\operatorname{ord}_m \mathfrak{A}_r - W_{i-r} \leqslant \operatorname{ord}_m L_j \neq \infty \quad (1 \leqslant j \leqslant k \ , \ 0 \leqslant m \leqslant M).$$

Through Lemma 1 we can choose integers $\lambda_1,\dots,\lambda_k$ such that

$$Q_{i+1} = \lambda_1 L_1 + \dots + \lambda_k L_k$$

does not lie in any $\mathfrak{p}_1,\dots,\mathfrak{p}_k$, and moreover $\deg Q_{i+1} \leqslant D_{i+1}$,

$$\operatorname{ord}_m \mathfrak{A}_r - W_{i-r} \leqslant \operatorname{ord}_m Q_{i+1} \neq \infty \qquad (0 \leqslant m \leqslant M).$$

Thus $\mathcal{B}_{i+1} = (Q_1,\dots,Q_{i+1})$ satisfies (10) with i replaced by i+1. We must now check (8) and (9). The construction of Q_{i+1} guarantees that

$$\mathcal{B}_i^{(m)} : Q_{i+1} = \mathcal{B}_i^{(m)} \qquad (0 \leqslant m \leqslant M). \tag{14}$$

So we conclude from (8) and Krull's Principal Ideal Theorem [5-I, p.238] that

$$\operatorname{rank} \mathcal{B}_{i+1}^{(m)} = i+1,$$

which verifies (8) for i+1. By (14) we also have $\mathcal{B}_i^* : Q_{i+1} = \mathcal{B}_i^*$. So by Proposition 4A of the appendix we have

$$\deg \mathcal{B}_{i+1}^* \leqslant \deg(\mathcal{B}_i^*, Q_{i+1}) \leqslant (D_1 \dots D_i) D_{i+1} ,$$

which verifies (9) for i+1. Therefore Proposition 5 follows.

V. PROOF FOR $r < n$.

Without affecting the validity of the assertion, we may, as in the proof of the case $n = r$, reindex $\theta_0, \ldots, \theta_M$ and decrease M if necessary to insure that each

$$\mathrm{ord}_m \mathcal{Q} > \begin{cases} (dT)^{2^{n-r-1}} & \text{if } d > 1 \\ (n-r) D_1^{n-r-1} T & \text{if } d = 1, \end{cases} \qquad . \; (0 < m < M).$$

Consider the primary decomposition of the ideal $\mathcal{B}_n^*$ produced by Propositions 3 and 5 :

$$\mathcal{B}_n^* = \mathfrak{q}_0 \cap \ldots \cap \mathfrak{q}_N .$$

Since rank $\mathcal{B}_n^* = n$ and $\mathrm{ord}_m \mathcal{B} > 0$ for each $0 < m < M$, it follows from Proposition 4 that $N = M$ and, after renumbering if necessary, the associated primes can be taken to be precisely $\mathfrak{m}_\theta, \ldots, \mathfrak{m}_M$. By (3),

$$\mathrm{ord}_m \mathcal{B}_n = \mathrm{ord}_m \mathcal{B}_n^* = \mathrm{ord}_m \mathfrak{q}_m \qquad (0 < m < M).$$

By Proposition 4 we know that

$$\mathrm{ord}_m \mathfrak{q}_m < \deg \mathfrak{q}_m .$$

From Proposition 3A of the appendix we see that

$$\sum_{m=o}^{M} \deg \mathfrak{q}_m = \deg \mathcal{B}_n^* .$$

Finally Proposition 5 furnishes the inequalities

$$\deg \mathcal{B}_n^* < D_1 \ldots D_n$$

and

$$\mathrm{ord}_m \mathcal{Q}_r < \mathrm{ord}_m \mathcal{B}_n + W_{n-r-1} .$$

Putting this all together with Proposition 3 gives

$$\begin{aligned}\sum_{m=o}^{M} \operatorname{ord}_m \mathfrak{a} = \sum_{m=o}^{M} \operatorname{ord}_m \mathfrak{a}_r &< \sum_{m=o}^{M} \operatorname{ord}_m \mathfrak{b}_n + (M+1)W_{n-r-1} \\ &< \sum_{m=o}^{M} \operatorname{ord}_m \mathfrak{g}_m + (M+1)W_{n-r-1} \\ &< \sum_{m=o}^{M} \deg \mathfrak{g}_m + (M+1)W_{n-r-1} \\ &< \deg \mathfrak{b}^*_n + (M+1)W_{n-r-1} \\ &< D_1 \ldots D_n + (M+1)W_{n-r-1} .\end{aligned}$$

This establishes the theorem after some straightforward computations.

We remark that the theorem applies to formal power series solutions of (1) over any field of characteristic zero.

APPENDIX.

Inhomogeneous Hilbert Functions

Recall that for a homogeneous ideal $\mathfrak{h}$ in K $[x_0,\ldots,x_n]$, where K is an infinite field, the associated volume function $V(t, \mathfrak{h})$ counts the number of K-linearly independent forms of degree t in $\mathfrak{h}$ [2,pp.154-162] . The Hilbert characteristic function of $\mathfrak{h}$ is given by

$$H(t, \mathfrak{h}) = \binom{n+t}{n} - V(t, \mathfrak{h}).$$

$H(t, \mathfrak{h})$ counts the number of K- linearly independent forms of degree t modulo $\mathfrak{h}$.

Similarly for an arbitrary ideal $\mathfrak{a}$ of $K[x_1,\ldots,x_n]$, the associated affine volume function $V_a(t, \mathfrak{a})$ counts the number of K-linearly independent polynomials in $\mathfrak{a}$ of degree at most t [2,p.157] . The affine characteristic function of $\mathfrak{a}$, $H_a(t,\mathfrak{a})$, counts the number of K-linearly independent polynomials modulo $\mathfrak{a}$ of degree at most t in K $[x_1,\ldots,x_n]$, and so

$$H_a(t, \mathfrak{a}) = \binom{n+t}{n} - V_a(t, \mathfrak{a}).$$

The parallel with the usual characteristic function is obviously strong, but still one cannot carry over the standard proofs to the affine case in a straightforward way.

The following basic property of $V(t,\mathfrak{h})$ comes from the fact that the dimensions of the sum and intersection of a pair of vector subspaces add up to the sum of the dimensions of the original subspaces : for homogeneous ideals $\mathfrak{h}$, $\mathfrak{k}$

$$V(t,\mathfrak{h}) + V(t,\mathfrak{k}) = V(t,\mathfrak{h}+\mathfrak{k}) + V(t,\mathfrak{h}\cap\mathfrak{k}).$$

However for affine ideals $\mathfrak{a}$, $\mathfrak{b}$ one has merely

$$V_a(t,\mathfrak{a}) + V_a(t,\mathfrak{b}) < V_a(t,\mathfrak{a}+\mathfrak{b}) + V_a(t,\mathfrak{a}\cap\mathfrak{b}).$$

For example, when we set $\mathfrak{a} = (x^2+1)$, $\mathfrak{b} = (x^2)$ in $K[x]$, then $\mathfrak{a}+\mathfrak{b} = K[x]$ and $\mathfrak{a}\cap\mathfrak{b} = (x^4+x^2)$. So for $t = 2$, $V_a(2,\mathfrak{a}) = V_a(2,\mathfrak{b}) = 1$, $V_a(2,\mathfrak{a}+\mathfrak{b}) = 3$, and $V_a(2,\mathfrak{a}\cap\mathfrak{b}) = 0$.

In spite of this divergence of behavior, one can still deduce from many of the properties of $H(t,\mathfrak{h})$ the corresponding ones for $H_a(t,\mathfrak{a})$. Now the map

$$f(x_1,\dots,x_n) \longmapsto x_0^t f(x_1/x_0,\dots,x_n/x_0)$$

is a K-vector space isomorphism between the subspace of polynomials of degree at most t lying in an ideal $\mathfrak{a}$ and the subspace of the corresponding graded ideal ${}^{gr}\mathfrak{a}$ consisting of forms of degree t. Since ${}^{gr}\mathfrak{a}$ is made up of all forms of the corresponding homogeneous ideal ${}^{h}\mathfrak{a}$, we see that

(15) $$V_a(t,\mathfrak{a}) = V(t,{}^{h}\mathfrak{a}), \quad H_a(t,\mathfrak{a}) = H(t,{}^{h}\mathfrak{a}).$$

In particular we have the following result :

THEOREM 1A : The characteristic function of an ideal $\mathfrak{a}$ in $K[x_1,\dots,x_n]$ of rank r has the following representation for large enough values of t in terms of binomial coefficients :

$$H_a(t,\mathfrak{a}) = h_0\binom{t}{n-r} + h_1\binom{t}{n-r-1} + \dots + h_{n-r}$$

with $h_0,\dots,h_r$ in Z and $h_0 > 0$.

We call h_0 the degree of $\mathfrak{a}$ and write also $h_0(\mathfrak{a})$. The theorem follows from (15) and the corresponding representation for $H(t,{}^h\mathfrak{a})$ [2,p.161] .

Recall that if $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_N$ is an irredundant primary decomposition with associated prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_N$, respectively, then ${}^h\mathfrak{a} = {}^h\mathfrak{q}_1 \cap \dots \cap {}^h\mathfrak{q}_N$ is also an irredundant primary decomposition with associated primes ${}^h\mathfrak{q}_1, \dots, {}^h\mathfrak{q}_N$ [5-II, p.181] . Note also that the homogeneous ideals which are equivalent to their dehomogenized ideals are those whose prime components do not contain x_0 [5-11, p.184] .

Proposition 2A : The degree of a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ of length ℓ satisfies

$$h_0(\mathfrak{q}) = h_0(\mathfrak{p}).$$

Proof : Since the map $\mathfrak{a} \to {}^h\mathfrak{a}$ is injective [5-II,p.182] , the homogenization of a maximal chain of $\mathfrak{p}$-primary ideals

$$\mathfrak{q} = \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_\ell = \mathfrak{p}$$

is a maximal chain of ${}^h\mathfrak{p}$-primary ideals lying above ${}^h\mathfrak{q}$. Now the claim follows from the corresponding property for homogeneous ideals [2, p.166] .

The following result is obtained similarly :

Proposition 3A : Let $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s \cap \mathfrak{q}_{s+1} \cap \dots \cap \mathfrak{q}_t$ be an irredundant primary decomposition where rank $\mathfrak{a}$ = rank $\mathfrak{q}_1$ = ... = rank $\mathfrak{q}_s$, but rank $\mathfrak{q}_{s+1}, \dots,$ rank $\mathfrak{q}_t$ are larger. Then

$$h_0(\mathfrak{a}) = h_0(\mathfrak{q}_1) + \dots + h_0(\mathfrak{q}_s)$$

Proposition 4A : Let $\mathfrak{a}$ be unmixed, rank $\mathfrak{a} \leqslant n-1$ and let f be a polynomial of degree $D \geqslant 1$ such that $\mathfrak{a} : (f) = \mathfrak{a}$ and $\mathfrak{a} + (f) \neq K[x_1, \dots, x_n]$. Then

$$\begin{aligned} \text{rank } \mathfrak{a} + (f) &= 1 + \text{rank } \mathfrak{a}, \\ h_0(f) &= D, \end{aligned}$$

and

$$h_0(\mathfrak{a} + (f)) < Dh_0(\mathfrak{a})$$

<u>Proof</u> : The first assertion follows from Krull's Principal Ideal Theorem [3,p.37], [5-I, p.238] . The second assertion holds for any non-zero polynomial and follows from the corresponding property for homogeneous polynomials [2,p.167] .

For the final assertion note that $\mathfrak{a} : (f) = \mathfrak{a}$ is equivalent to saying that f does not lie in any prime ideals associated with $\mathfrak{a}$. This property remains true under homogenization. Since ${}^h\mathfrak{a} + ({}^hf) \subsetneq {}^h(\mathfrak{a} + (f))$, we find

$$H_a(t, \mathfrak{a} + (f)) < H(t, {}^h\mathfrak{a} + ({}^hf)).$$

So when we apply the Bezout theorem for homogeneous ideals [3, p.64] or [2,p.167] , we obtain the desired inequality. Let us finally note that every time we use Proposition 4.A, the positivity of the orders of $\mathfrak{a}$ and f enables us to verify the condition that $\mathfrak{a} + (f) \neq \mathbb{C}[x_1, \dots, x_n]$.

<u>BIBLIOGRAPHY</u>

[1] W. D. Brownawell and D. W. Masser, Multiplicity estimates for analytic functions II.

[2] W. Gröbner, Moderne Algebraische Geometrie, die idealtheoretischen Grundlagen, Springer Verlag, Wien und Innsbruck, 1949.

[3] W. Krull, Idealtheorie, 2nd expanded printing, Springer Verlag, Berlin, 1968.

[4] Ju. V. Nesterenko, Estimates for the orders of zero of some functions of a certain class and their application in the theory of transcendental numbers, Izv. Akad. Nauk SSR, Ser. Mat. 41 (1977), 253-284, Math. USSR Izv. 11 (1977), 239-279, (see also these Proceedings).

[5] O. Zariski and P. Samuel, Commutative Algebra, Volumes I and II, Springer Verlag, New York, 1968.

The Pennsylvania State University
Department of Mathematics
215, Mc Allistair Building
University Park, Penn. 16802
U. S. A.

MÉMOIRES DE LA S. M. F.

G. V. CHUDNOVSKY

Constructive and non-constructive methods of proofs of irrationality and transcendency and algebraic independence of periods of abelian varieties

Mémoires de la S. M. F. 2e série, tome 2 (1980), p. 21-22

<http://www.numdam.org/item?id=MSMF_1980_2_2__21_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 21-22

CONSTRUCTIVE AND NON-CONSTRUCTIVE METHODS OF PROOFS OF IRRATIONALITY AND TRANSCENDENCY AND ALGEBRAIC INDEPENDENCE OF PERIODS OF ABELIAN VARIETIES .

by G. V. Chudnovsky

The methods announced in the title are based on the deformation theory for Fuchsian linear differential equations. They include effective constructions of the Padé approximations to generalized hypergeometric functions giving the periods of certain algebraic varieties, of the Padé approximations to systems of Abelian integrals of the first and second kind, and of the Padé approximations to systems of Abelian functions on certain Abelian varieties. We shall describe the arithmetic structure of the coefficients of the polynomials in the Padé approximations, their sizes and the remainder term.

Example 1 : Let k be an algebraic number such that $0<|k|<1$, and consider the equation : $y^2=(1-x^2)(1-k^2x^2)$. If $|k|^2<(H(k^2))^{-\delta}$ for some positive δ, then

$$|x\pi+y\omega+z\eta|>H^{-C}$$

where $C=C(\delta)$.

If now $k^2=1/q$ and $q\geq q_0(\varepsilon)$, then

$$|x\pi+y\omega+z\eta|>H^{-3-\varepsilon} .$$

In these formulae, x, y, z are integers, $0<\max(|x|,|y|,|z|)=H$ and ω and η are respectively the period and quasi period of the corresponding elliptic curve.

The same type of result can be proved for n elliptic curves.

Example 2 : If $E: y^2 = 4x^3 - g_2x - g_3$ is defined over $\mathbb{Q}$ and $\wp(u) = 1/q$ for $q \geq q_0(\varepsilon)$, then

$$|u\wp'(u) - r/s| > |s|^{-2-\varepsilon}.$$

We obtain similar results, under much milder restrictions, for $\zeta(u) + \alpha u$, $\alpha \in \mathbb{Q}$, as well.

These are the most elementary examples. It should be noted that we can compute all the constants explicitly.

We shall also present results on algebraic independence for sets of numbers connected with the exponential function and Abelian functions. We propose new bounds for the types of transcendence of two numbers, as η/ω and $\zeta(u) - (\eta/\omega)u$, the algebraic independence of which was earlier proved by the author . Finally, we consider an elliptic function $\wp(z)$ with complex multiplication over K, and obtain the bound

$$|P(\wp(\alpha),\wp(\beta)| > H(P)^{-C_2 d(P)^2}$$

where $\log\log H(P) \geq d(P)^4$ and $C_2 = C_2([K(\alpha,\beta):\mathbb{Q}]) > 0$.

Institut des Hautes Etudes Scientifiques
35, route de Chartres
91440 Bures-sur-Yvette
(France)

Mémoires de la S. M. F.

Pierre Deligne

Cycles de Hodge absolus et périodes des intégrales des variétés abéliennes. (Rédigé par J. L. Brylinski)

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 23-33

<http://www.numdam.org/item?id=MSMF_1980_2_2__23_0>

SOCIETÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 23-33

CYCLES DE HODGE ABSOLUS ET PÉRIODES DES INTÉGRALES DES VARIÉTÉS ABÉLIENNES

par

Pierre DELIGNE

rédigé par J. L. BRYLINSKI

On montre ici comment une théorie convenable des "motifs" permet de retrouver certains des résultats de Shimura sur les périodes des variétés abéliennes de type C-M [5] . Il a paru instructif de commencer par une description informelle des propriétés des motifs et de leurs réalisations : c'est ce qui est fait au paragraphe 1. Le paragraphe 2 interprète certains résultats de Shimura à l'aide de motifs. Le paragraphe 3 définit les cycles de Hodge absolus, et la théorie des motifs qui leur est subordonnée. Le paragraphe 4 donne une majoration du degré de transcendance du corps engendré par les périodes d'une variété abélienne quelconque.

§ 1. LE LANGAGE DES MOTIFS

Soit k un corps de caractéristique 0. Il existe des "motifs sur k" plusieurs définitions, dont on ignore si elles sont équivalentes, et ayant chacune leurs vertus. Nous préciserons au paragraphe 3 laquelle nous est utile.

Les motifs sur k forment une catégorie additive, munie d'un produit tensoriel. Chaque variété projective et lisse X sur k définit un motif h(X) sur k, la cohomologie motivique de X, et tout motif sur k se déduit d'un motif de cette forme (par découpage en morceaux et twist à la Tate). Enfin, à diverses théories de cohomologie pour les variétés algébriques correspondent des foncteurs "réalisation" pour les motifs.

Chaque variété abélienne A sur k définit un motif T(A) sur k, son H_1 motivique, et le foncteur $A \mapsto T(A)$ est pleinement fidèle. Plonger la catégorie des variétés abéliennes dans celle des motifs a pour intérêt de pouvoir prendre des $\otimes$. Mais les objets obtenus ne sont pas géométriques : il n'y a pas de "fonctions" sur un motif.

Le rang d'un motif est la dimension de l'une quelconque de ses réalisations, que nous allons maintenant décrire.

Si $k = \mathbb{C}$, la réalisation de Betti d'un motif M est un groupe abélien libre de rang fini $H_B(M)$, qui est muni d'une structure de Hodge, c'est-à-dire d'une décomposition :

$$H_B(M) \otimes_{\mathbb{Z}} \mathbb{C} = \bigoplus_{p+q=n} H^{p,q} \quad (\text{avec } \bar{H}^{p,q} = H^{q,p}) .$$

Illustrons ceci sur le motif T(A), qui est le H_1 d'une variété abélienne A. On définit $H_B(T(A)) = H_1(A,\mathbb{Z})$, homologie de $A = A(\mathbb{C})$ vu comme espace topologique. Soit Lie (A) l'algèbre de Lie du groupe analytique A, et soit $\int : H_1(A,\mathbb{Z}) \to \mathrm{Lie}(A)$ l'homomorphisme "intégration sur un 1-cycle". On a une suite exacte de groupes analytiques complexes :

$$0 \longrightarrow H_1(A,\mathbb{Z}) \xrightarrow{\int} \mathrm{Lie}\ (A) \xrightarrow{\exp} A \longrightarrow 0$$

La structure de Hodge de $H_1(A,\mathbb{C})$ est telle que $H_1(A,\mathbb{C}) = H^{0,-1} \oplus H^{-1,0}$. On obtient $H^{0,-1}$ comme noyau de l'application $H_1(A,\mathbb{C}) \to \mathrm{Lie}\ (A)$, prolongement $\mathbb{C}$-linéaire de

$\int : H_1(A,\mathbb{Z}) \to \mathrm{Lie}(A)$.

Plaçons-nous maintenant sur un corps de caractéristique 0 et donnons-nous une clôture algébrique $\bar{k}$ de k.. Pour tout nombre premier ℓ , la réalisation ℓ -adique d'un motif M est un $\mathbb{Z}_\ell$-module libre de type fini $H_\ell(M)$ (muni d'ailleurs d'une action du groupe de Galois de $\bar{k}$ sur k). Lorsque k = ℂ, on dispose d'un isomorphisme : $H_\ell(M) \cong H_B(M) \otimes \mathbb{Z}_\ell$. Si A est une variété abélienne sur k, si $\bar{k}$ est une clôture algébrique de k, la réalisation ℓ-adique de T(A) est notée $T_\ell(A)$; c'est le $\mathbb{Z}_\ell$-module :

$$T_\ell(A) = \varprojlim_n A_{\ell^n}(\bar{k})$$ (où $A_{\ell^n}(\bar{k})$ est le groupe des points d'ordre ℓ^n de $A(\bar{k})$).

Si k = ℂ, l'isomorphisme $T_\ell(A) \cong H_B(T(A)) \otimes \mathbb{Z}_\ell$ est facile à décrire. Pour tout n, la projection de $\gamma \otimes x \in H_B(T(A)) \otimes \mathbb{Z}_\ell$ sur $A_{\ell^n}(\mathbb{C})$ se calcule ainsi ; si $m \in H_B(T(A))$ est tel que $x - m \in \ell^n(H_B(T(A)) \otimes \mathbb{Z}_\ell)$, l'exponentielle de l'élément $\frac{m}{\ell^n} \in H_1(A,\mathbb{Q})$ est le point d'ordre ℓ^n voulu.

La réalisation de De Rham de M est un espace vectoriel sur k de dimension finie $H_{DR}(M)$, muni d'une filtration décroissante $F^\bullet$(la filtration de Hodge). Lorsque k = ℂ , on a un isomorphisme $H_B(M) \otimes \mathbb{C} \simeq H_{DR}(M)$. Par cet isomorphisme, la filtration de Hodge est telle que $F^p = \bigoplus_{p' \geq p} H^{p',q}$. Dans le cas du motif T(A), rappelons [7] l'existence d'une "extension universelle" E de A par un groupe vectoriel, qui s'inscrit dans une suite exacte de groupes algébriques : $0 \to H^1(A,\mathcal{O}_A)^* \to E \to A \to 0$. On a $H_{DR}(T(A) = \mathrm{Lie}(E)$, et la filtration de Hodge est donnée par :

$$0 = F^1 \subset F^0 = H^1(A,\mathcal{O}_A)^* \subset F^{-1} = \mathrm{Lie}(E)$$

Si k = ℂ, on a $H_1(E,\mathbb{Z}) \xrightarrow{\sim} H_1(A,\mathbb{Z})$, d'où un morphisme :

$H_1(A,\mathbb{C}) \xrightarrow{\sim} H_1(E,\mathbb{C}) \xrightarrow{\int} \mathrm{Lie}(E) = H_{DR}(T(A))$. C'est l'isomorphisme voulu.

Exemples : 1) Ici, $k = \mathbb{Q}$. On va définir le motif de Tate $\mathbb{Z}(1)$; c'est le H_1 du groupe algébrique $\mathbb{G}_m$. Pour trouver ses diverses réalisations, on substitue $\mathbb{G}_m$ à A dans la définition de T(A). On obtient :

- $H_B(\mathbb{Z}(1)) = 2\pi i.\mathbb{Z}$, noyau de $\exp : \mathbb{C} \longrightarrow \mathbb{C}^\times$
  $H_B(\mathbb{Z}(1)) \otimes \mathbb{C} = H^{-1,-1}$
- $H_\ell(\mathbb{Z}(1)) = \mathbb{Z}_\ell(1) = T_\ell(\mathbb{G}_m) = \varprojlim_n \mu_{\ell^n}(\bar{\mathbb{Q}})$
- $H_{DR}(\mathbb{Z}(1)) = \mathbb{Q}$.

L'isomorphisme $H_B(\mathbb{Z}(1)) \otimes \mathbb{C} \xrightarrow{\approx} H_{DR}(\mathbb{Z}(1)) \otimes \mathbb{C}$ envoie $(2\pi i) \otimes 1$ sur $2\pi i$. On rappelle les isomorphismes $H_1(\mathbb{G}_m) \cong H_1(\mathbb{P}^1 - \{0,\infty\}) \cong H_2(\mathbb{P}^1)$. De plus , pour toute courbe algébrique propre lisse et connexe sur $\mathbb{Q}$, $H_2(X)$ est isomorphe à $H_2(\mathbb{P}^1)$ (donc à $\mathbb{Z}(1)$) .Pour tout entier d, on définit un motif $\mathbb{Z}(d)$ de sorte que $\mathbb{Z}(d) = \mathbb{Z}(d-1) \otimes \mathbb{Z}(1)$. On a $\mathbb{Z}(m+n) = \mathbb{Z}(m) \otimes \mathbb{Z}(n)$ pour $m, n \in \mathbb{Z}$.

2) Soit E une courbe elliptique sur $\mathbb{Q}$. Le motif T(E) est de rang 2. Donc le motif $\Lambda^2 T(E)$ est de rang 1, et on a $\Lambda^2 T(E) = \Lambda^2 H_1(E) = H_2(E) = \mathbb{Z}(1)$. Précisons l'isomorphisme $\Lambda^2 T(E) \cong \mathbb{Z}(1)$ dans les différentes réalisations. Sur $H_1(E(\mathbb{C}),\mathbb{R}) \simeq$ Lie (E), la structure complexe définit une orientation. Si (e_1,e_2) est une $\mathbb{Z}$-base orientée de $H_B(T(E)) = H_1(E(\mathbb{C}),\mathbb{Z})$, alors $e_1 \wedge e_2$ est une base de $H_B(\Lambda^2 T(E))$; on lui associe $2\pi i \in H_B(\mathbb{Z}(1))$.

L'isomorphisme $\Lambda^2(T_\ell(E)) \cong \mathbb{Z}_\ell(1)$ est donné par la forme alternée de Weil [6] . Enfin, on a : $\Lambda^2 H_{DR}(T(E)) = \mathrm{Hom}(H^2_{DR}(E),\mathbb{Q})$. Soient ω et η les formes différentielles habituelles de première et deuxième espèce. $H^2_{DR}(E)$ est engendré par le cup-produit $\omega \wedge \eta$ de leurs classes de cohomologie. Par l'isomorphisme $H_B(\Lambda^2 T(E)) \otimes \mathbb{C} \to H_{DR}(\Lambda^2 T(E)) \otimes \mathbb{C}$, $e_1 \wedge e_2$ a pour image l'homomorphisme qui envoie $\omega \wedge \eta \in H^2_{DR}(E)$ sur $\begin{vmatrix} \omega_1 & \omega_2 \\ \eta_1 & \eta_2 \end{vmatrix} \in \mathbb{C}$. La compatibilité des réalisations de Betti et de De Rham de l'isomorphisme $\Lambda^2(T(E)) \cong \mathbb{Z}(1)$ équivaut à la relation de Legendre

$$\omega_1 \cdot \eta_2 - \omega_2 \cdot \eta_1 = 2\pi i$$

3) Soit A une variété abélienne sur $\mathbb{Q}$. A la classe de cohomologie d'une section hyperplane de A dans un plongement projectif, correspond un morphisme de motifs $\Lambda^2 T(A) \to \mathbb{Z}(1)$. En cohomologie de Betti, ceci correspond à une forme alternée $2\pi i.E$ sur $H_B T(A)$, à valeurs dans $2\pi i.\mathbb{Z}$. En cohomologie de De Rham, on a de même une forme alternée E_{DR} sur $H_{DR}(T(A))$ à valeurs dans $\mathbb{Q}$. Il est classique que F^o est un sous-espace totalement isotrope. On en déduit qu'on peut trouver des différentielles de première espèce $\omega_1,\dots,\omega_g$ sur A, des différentielles de deuxième espèce $\eta_1,\dots,\eta_g$ sur A, telles que l'on ait :

$E_{DR}(x,y) = \sum_{i=1}^{g} (\omega_i,x)(\eta_i,y) - (\omega_i,y).(\eta_i,x)$. La compatibilité entre E et E_{DR} se traduit comme suit. Soit $(e_1,\dots,e_{2g})$ une base de $H_B(T(A))$, soit Ω la matrice $n \times 2n$ telle que $\Omega_{ij} = \int_{e_j} . \omega_i$, et N la matrice $n \times 2n$ telle que $N_{ij} = \int_{e_j} \eta_i$. On a :

$$^tN.\Omega - {}^t\Omega .N = 2i\pi .E \ .$$

Enfin, pour la réalisation ℓ -adique on trouve une forme alternée sur $T_\ell(A)$ à valeurs dans $\mathbb{Z}_\ell(1)$: c'est la forme alternée de Weil associée au diviseur de la section hyperplane [6].

§ 2. MOTIFS LIÉS AUX VARIÉTÉS ABÉLIENNES DE TYPE C-M

Soit k un sous-corps algébriquement clos de $\mathbb{C}$ - par exemple $\bar{\mathbb{Q}}$- et soit $\mathcal{A}$ la sous-catégorie de la catégorie des motifs sur k, engendrée par les T(A) des variétés abéliennes (pour les opérations de produit tensoriel, passage au dual et facteurs directs). Le foncteur "réalisation de Betti de motif déduit de M/k par extension des scalaires à $\mathbb{C}$" envoie $\mathcal{A}$ dans la catégorie des structures de Hodge. Il résulte formellement du Théorème 1 du § 3 que ce foncteur est pleinement fidèle.

Soient E un corps CM, S l'ensemble de ces plongements complexes et $- : S \to S$ la conjugaison complexe. A chaque fonction $\varphi : S \to \mathbb{Z}$ vérifiant

$$(*)\quad \varphi(\sigma) + \varphi(\bar{\sigma}) \text{ est indépendant de } \sigma \in S,$$

attachons une structure de Hodge H_φ , munie d'une structure de module sur l'anneau $\mathcal{O}_E$ des entiers de E :

$H_\varphi = \mathcal{O}_E$, muni de la structure de module évidente, et dans la décomposition $H_\varphi \otimes \mathbb{C} = E \otimes \mathbb{C} \rightarrow \mathbb{C}^S$, le facteur $\mathbb{C}$ d'indice $\sigma \in S$ est de type de Hodge $(\varphi(\sigma),\ \varphi(\bar{\sigma}))$.

On vérifie que les H_φ sont dans l'image de $\mathcal{A}$, et même dans l'image de la sous-catégorie engendrée par les variétés abéliennes de type CM. Ceci permet de définir le motif M_φ sur $\bar{\mathbb{Q}}$ comme étant celui de réalisation de Betti H_φ .

La réalisation de De Rham $H_{DR}(M_\varphi)$ est un espace vectoriel sur $\bar{\mathbb{Q}}$, muni d'une action de E. Pour tout $\sigma \in S$, soit $H_{DR}(M_\varphi)_\sigma$ le sous $\bar{\mathbb{Q}}$-espace vectoriel sur lequel $x \in E$ agit comme $\sigma^{-1}(x) \in \bar{\mathbb{Q}}$. Chacun de ces espaces vectoriels est de dimension 1 engendré par un élément ω_σ , et $H_{DR}(M_\varphi)$ en est la somme . Via l'isomorphisme : $H_B(M_\varphi) \otimes \mathbb{C} \xrightarrow{\approx} H_{DR}(M_\varphi) \otimes \mathbb{C}$, un élément e de $E = H_B(M_\varphi) \otimes \mathbb{Q}$ correspond à une famille (e_σ) avec $e_\sigma \in H_{DR}(M_\varphi)_\sigma$. On vérifie immédiatement que le nombre complexe $p(\sigma,\varphi)$ tel que $p(\sigma,\varphi).e_\sigma = \omega_\sigma$ ne dépend à multiplication près par $\bar{\mathbb{Q}}^X$, ni de e ni du choix de ω_σ . Ceci justifie la notation. Entre les $p(\sigma,\varphi)$ et les <u>invariants de Shimura</u> $p_E(\sigma,\varphi)$ (voir [5]), on a la relation :

$$p_E(\sigma,\varphi) = \frac{p(\sigma,\varphi)}{(2\pi i)^{\varphi(\sigma)}} \text{ (modulo } \bar{\mathbb{Q}}^X)$$

(qui n'est qu'une traduction des définitions).

Les identités entre les périodes de Shimura, correspondent à des propriétés algébriques des motifs M . Avant de les résumer en un tableau, introduisons quelques notations relatives à une extension F|E de corps CM. On note S_F(resp.S_E) l'ensemble des plongements complexes de F (resp. E). Pour $\sigma \in S_F$, on note $\sigma|E \in S_E$ la restriction à E du plongement σ .

Pour $\varphi : S_E \to \mathbb{Z}$ satisfaisant (*), on note $\mathrm{Inf}(\varphi)$ la fonction de S_F vers $\mathbb{Z}$ telle que $\mathrm{Inf}(\varphi)(\sigma) = \varphi(\sigma|E)$. Cette fonction satisfait (*). Pour $\varphi : S_F \to \mathbb{Z}$ satisfaisant (*), on note $\mathrm{Res}(\varphi)$ la fonction de S_E vers $\mathbb{Z}$ telle que $\mathrm{Res}(\varphi)(\sigma) = \sum\limits_{\tau|E=\sigma} (\tau)$; elle satisfait (*).

Identités entre périodes	Relations entre motifs
1. $p(\sigma,\varphi'+\varphi'') = p(\sigma,\varphi').p(\sigma,\varphi'')$	1. $M_{\varphi'+\varphi''} = M_{\varphi'} \otimes_E M_{\varphi''}$
2. F|E extension de corps CM, $\sigma \in S_F$ $\varphi : S_E \to \mathbb{Z}$ satisfaisant (*) : $p(\sigma,\mathrm{Inf}(\varphi)) = p(\sigma|E,\varphi)$	2. $M_{\mathrm{Inf}(\varphi)} = M_\varphi \otimes_E F$
3 $\sigma \in S_E$, $\varphi : S_F \to \mathbb{Z}$ satisfaisant (*) : $p(\sigma,\mathrm{Res}\,\varphi) = \prod\limits_{\tau|E=\sigma} p(\tau,\varphi)$	3. M_φ est un F-motif de rang 1, donc un E-motif de rang $d = [F:E]$ $M_{\mathrm{Res}(\varphi)} = \Lambda^d_E M_\varphi$
4. $p(\sigma,\underline{1}) = 2\pi i$	4. $M_{\underline{1}} = \mathbb{Z}(-1)$ (dual du motif de Tate)

Ces identités entre périodes permettent de retrouver les théorèmes 1 à 4 de l'exposé de Shimura [5]. Notons que dans [5] Shimura relie les périodes $p_K(\sigma,\varphi)$ aux valeurs en un point spécial de formes modulaires de Hilbert, rationnelles sur $\bar{\mathbb{Q}}$.

§ 3. CYCLES DE HODGE ABSOLUS ET MOTIFS

Soit X une variété projective et lisse sur $\mathbb{C}$. Un cycle de Hodge de codimension d sur X est un élément de $H^{2d}(X,\mathbb{Q})$ de type (d,d), ou, ce qui revient au même, un élement de $H^{2d}(X,\mathbb{Q})(d) \overset{\mathrm{def}}{=} H^{2d}(X,\mathbb{Q}) \otimes \mathbb{Z}(d)$ de type (0,0). Remarquons que pour $x \in H^{2d}(X,\mathbb{Q})(d)$, il est équivalent de dire que x est de type (0,0) ou que x est dans F^0. Une classe de cohomologie d'une sous-variété algébrique de X est un cycle de Hodge. Hodge a conjecturé que tout cycle de Hodge serait combinaison linéaire de classes de cohomologie de sous-variétés. Cette conjecture paraissant inaccessible, on introduit une notion qui "arithmétise" celle de cycle de Hodge. Les cycles qu'on définit auront tous les attributs visibles des cycles algébriques, à savoir des réalisations en cohomologie ℓ-adiques et de De Rham. Un <u>cycle de Hodge absolu</u> de codimension d sur une variété projective lisse X, sur un corps k de caractéristique O, sera une collection de classes de cohomologie dans les groupes $H^{2d}(X,\mathbb{Q}_\ell)(d)$ (resp. $H^{2d}_{DR}(X)(d)$) satisfaisant les deux conditions

- l'élément de $H^{2d}_{DR}(X)(d)$ est dans F^o ;
- pour tout plongement $k \xhookrightarrow{\tau} \mathbb{C}$, les différentes classes de cohomologie correspondent (via les isomorphismes du § 1) à <u>une</u> classe rationnelle de la cohomologie de Betti de $X \otimes_k \mathbb{C}$.

On a les inclusions : (cycles algébriques) $\subset$ (cycles de Hodge absolus) $\subset$ (cycles de Hodge). Utilisons cette définition pour préciser la catégorie des motifs sur laquelle on a travaillé dans les § 1 et 2. Soit d'abord $\mathcal{V}(k)$ la catégorie des variétés projectives et lisses sur k. On construit une catégorie <u>additive</u> $\mathcal{M}(k)$, dans laquelle les groupes Hom(M,N) sont des espaces vectoriels sur $\mathbb{Q}$, qui est munie des données suivantes :

a) un produit tensoriel $\otimes$, associatif, commutatif, distributif par rapport à l'addition des objets

b) un foncteur contravariant H^* de $\mathcal{V}(k)$ dans $\mathcal{M}(k)$, bijectif sur les objets, compatible aux sommes, transformant produits en produits tensoriels.

Dans $\mathcal{M}(k)$, on a, pour X et Y connexes :
$\mathrm{Hom}(H^*(X),H^*(Y)) = Z^{\dim(Y)}_{h.a}(X \times Y)$, où on note $Z^d_{h.a}(Z)$ l'espace vectoriel sur $\mathbb{Q}$ des cycles de Hodge absolus de codimension d sur Z. La construction de la catégorie de motifs $\mathcal{M}(k)$ se fait alors tout comme dans [2], les cycles algébriques étant remplacés par les cycles de Hodge absolus. Grâce à cette nouvelle définition, les composantes de Künneth de la diagonale de X × X étant de Hodge absolues, on a dans $\mathcal{M}(k)$ une décomposition : $H^*(X) = \bigoplus_i H^i(X)$.

CYCLES DE HODGE ET PÉRIODES

Le résultat qui suit a fait l'objet d'exposés à l'I. H. E. S. en 1979.

Théorème 1 : *Tout cycle de Hodge sur une variété abélienne est de Hodge absolu.* Signalons le

Corollaire (Borovoï) : *Soit* A *une variété abélienne sur un corps* k *de caractéristique* O, ξ *un cycle de Hodge sur* A. *Les correspondants* ℓ-*adiques* ξ_ℓ *de* ξ *sont fixés par un sous-groupe ouvert de* $\mathrm{Gal}(\bar{k}|k)$.

§ 4. PÉRIODES DES INTÉGRALES DES VARIÉTÉS ABÉLIENNES

Soit A une variété abélienne complexe, $H_1(A,\mathbb{C}) = H^{0,-1} \oplus H^{-1,0}$ la décomposition de Hodge de $H_B(A)$ (cf. § 1). Considérons $GL(H_1(A))$ comme groupe algébrique sur $\mathbb{Q}$. On a un morphisme de groupes algébriques complexes : $\mathbb{G}_m \xrightarrow{\mu} GL(H_1(A,\mathbb{C}))$ tel que $\mu(z)$ agisse par l'homothétie de rapport z sur $H^{-1,0}$, par l'identité sur $H^{0,-1}$. Le *groupe de Hodge* G de A est l'adhérence de Zariski du sous-groupe $\mu(\mathbb{G}_m)$ de $GL(H_1(A))$. En d'autres termes, G est un sous-groupe algébrique sur $\mathbb{Q}$ de $GL(H_1(A))$. Une fonction régulière sur un ouvert de Zariski de G, et $\mathbb{Q}$-rationnelle, est nulle sur G si et seulement si elle est nulle sur $\mu(\mathbb{G}_m)$. On vérifie aisément que G contient les homothéties de $H_1(A)$. Voici une seconde description de G, très utile : on considère tous les tenseurs rationnels de type $(-\frac{N}{2}, -\frac{N}{2})$ dans les produits tensoriels $\otimes^N H_1(A)$. Alors G est le sous-groupe de $GL(H_1(A))$ formé des transformations linéaires g pour lesquelles il existe un scalaire μ tel que : $g.t = \mu^m t$, pour tout tenseur t de type (m,m). Enfin, on montre que G est le groupe qui fixe tous les cycles de Hodge absolus de type (0,0) dans les espaces de tenseurs mixtes sur $H_1(A)$ (mixtes = covariants et contravariants). Supposons maintenant A définie sur un sous-corps k de $\mathbb{C}$. Posons g = dim(A).

Théorème 2 : *Soit* $\omega_1,\dots,\omega_g$ *des différentielles de première espèce sur* A, $\eta_1,\dots,\eta_g$ *des différentielles de deuxième espèce sur* A, *telles que*

$(\omega_1,\dots,\omega_g,\ \eta_1,\dots,\eta_g)$ soit une base de $H^1_{DR}(A)$. Soit K le sous-corps de $\mathbb{C}$ engendré par k et par les périodes $\int_\gamma \omega_i$, $\int_\gamma \eta_i$ $(1 < i < g,\ \gamma \in H_1(A,\mathbb{Z}))$; le degré de transcendance de K sur k est majoré par la dimension de G.

Démonstration : K est le corps de rationalité de l'isomorphisme $H_{1,B}(A) \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\approx} H_{1,DR}(A) \otimes_k \mathbb{C}$ donné par " intégration" sur un cycle. Cet isomorphisme préserve les classes de cohomologie des cycles de Hodge absolus. Soit P la variété algébrique formée des isomorphismes qui ont cette propriété. De la définition de G, et du théorème 1 résulte que P est un espace principal homogène sous G, défini sur k, donc $\dim(P) = \dim(G)$. On conclut par le lemme suivant :

Lemme : Soit z un point de $A^N(\mathbb{C})$; le degré de transcendance de $k(z)$ sur k est égal à la dimension de la k-adhérence de Zariski de $\{z\}$;

C'est une tautologie. C.Q.F.D.

Remarque : De l'exemple 3 du § 1, résulte que $2\pi i \in K$. On peut d'ailleurs montrer que le degré de transcendance de K sur $k(2\pi i)$ est majoré par $\dim(G)-1$.

Corollaire : Avec les notations du Theorème 2, supposons de plus A simple de type C-M. Le degré de transcendance de K sur k est majoré par $g+1$.

Preuve : Il suffit de montrer : $\dim(G) < g+1$. Or $\mu(\mathbb{G}_m)$ commute à l'action sur $H_1(A,\mathbb{Q})$ du corps E. Il en résulte que G commute aussi à cette action, et que G est un tore algébrique. Par ailleurs G préserve, à un facteur près, la forme alternée associée à une section hyperplane (voir l'exemple 3 du § 1). D'où l'assertion.

Remarquons que, dans ce dernier cas, on dispose de la minoration suivante : $\dim(G) > 2 + \log_2(g)$, due à Ribet [3].

RÉFÉRENCES

[1] P. Deligne : Valeurs de fonctions L et périodes d'intégrales, in Proceedings of symposia in Pure Mathematics, Volume 33, 1978.

[2] M. Demazure : Exposé au séminaire Bourbaki n° 365, in Springer Lecture Notes, 180 (1971).

[3] K. Ribet : Division fields of abelian varieties with complex multiplications, dans ce volume.

[4] G. Shimura : On the derivatives of modular forms, Duke Math. Journal 44 (1977), 365-387.

[5] G. Shimura : The periods of abelian varieties with complex mutliplication and the special values of certain zeta functions, dans ce volume.

[6] A. Weil : Courbes algébriques et variétés abéliennes, Hermann 1971 (réimpression).

[7] A. Weil : Variétés abéliennes, in "Algèbre et Théorie des Nombres", Colloque international du C.N.R.S., 24, 1950, p.124-127.

P. Deligne
Institut des Hautes Etudes Scientifiques
91440 Bures-sur-Yvette

J.-L. Brylinski
Ecole polytechnique, Centre de Mathématiques
91128 Palaiseau cedex

MÉMOIRES DE LA S. M. F.

E. DOBROWOLSKI

On a question of Lehmer

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 35-39

<http://www.numdam.org/item?id=MSMF_1980_2_2__35_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 35-39

ON A QUESTION OF LEHMER

by

E. DOBROWOLSKI

Let f be a polynomial with integral coefficients. Define the measure of f by

$$M(f) = a \prod_{i=1}^{n} \max(1, |\alpha_i|)$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the zeros of f listed with proper multiplicity and a is the leading coefficient. D. H. Lehmer [5] asked whether for every $\varepsilon > 0$ there exists a monic polynomial f such that $1 < M(f) < 1+\varepsilon$.

P. E. Blanksby and H. L. Montgomery [1] and the present writer [2] obtained lower bounds for M(f) in terms of the degree of f. In this paper we give a lower bound for M(f) in terms of the number of non-zero coefficients of the polynomial f. The existence of such a bound (but not its form) has been announced by W. Lawton [4] .

Theorem 1 : *If* $F(z) \in \mathbb{Z}[z]$ *is an irreducible non-cyclotomic polynomial,* $F(z) \neq \pm z$, *then*

$$M(F) > 1 + \frac{\log 2e}{2e} \; \frac{1}{(k+1)^k}$$

where k *is the number of non-zero coefficients of* F.

The argument used in the proof gives the following corollary.

Corollary 1 : *If* F *is a product of different cyclotomic polynomials and* F *has at most* k *non-zero coefficients then*

$$\ell(F) < k^k + 1$$

where $\ell(F)$ *denotes the sum of absolute values of the coefficients of* F.

The omission of the assumption of irreducibility of the polynomial F in Theorem 1 leads to a more complicated situation. In the general case the present writer, W. Lawton and A. Schinzel [3] obtained the following result .

Theorem 2 : *If* $g(z) \in \mathbb{Z}[z]$ *is a monic polynomial with* $g(0) \neq 0$ *that is not a product a cyclotomic polynomials then*

$$M(g) > 1 + \frac{1}{\exp_{k+1} 2k^2}$$

where k *is the number of non-zero coefficients of* g.
(Here, $\exp_{k+1}$ denotes the $(k+1)$-th iterate of the exponential function).

In the proof we use notation of $\ell(f)$ and $M(f)$ as above. Further $|f|$ denotes the degree of f. For a vector $\underline{x}$, $\ell(\underline{x})$ denotes the sum of absolute values of coordinates of $\underline{x}$.

Lemma 1 : *If* α *is a non-zero algebraic integer of degree* n *which is not a root of unity, and if* p *is a prime number, then*

$$\left| \prod_{i,j=1}^{n} (\alpha_i^p - \alpha_j) \right| > p^n$$

Proof : This is Lemma 1 of [2] .

Lemma 2 : *If* $f(z) \in \mathbb{Z}[z]$ *is an irreducible polynomial and*

$$M(f) < 1 + \frac{\log 2e}{2e} \frac{1}{\ell(f)}$$

then f *is a cyclotomic polynomial* or $f(z) = \pm z$.

Proof : Let p be a prime number in the interval $e\ell(f) < p < 2e\ell(f)$. Suppose that f is not a cyclotomic polynomial and let $\alpha_1, \alpha_2, \ldots \alpha_{|f|}$ be its zeros. Lemma 1 gives

$$\ell(f)^{|f|} M(f)^{p|f|} \geq \left| \prod_{i=1}^{|f|} f(\alpha_i^p) \right| \geq p^{|f|}$$

which is inconsistent with the inequality assumed in the Lemma. This Lemma was also proved with $\frac{1}{6}$ in place of $\frac{\log 2e}{2e}$ by C. L. Stewart, M. Mignotte and M. Waldschmidt, see [6] .

Lemma 3 : *Let* $\underline{a} \in \mathbb{Z}^N$ *be a vector with* $\ell(\underline{a}) \geq (NB)^N + 1$ *and* $B > 1$ *be a real number*. *Then there exist vectors* $\underline{c} \in \mathbb{Z}^N$ *and* $\underline{r} \in \mathbb{Q}^N$ *and a rational number* q *such that*

(i) $\underline{a} = \underline{r} + q\,\underline{c}$

(ii) $0 \neq \ell(\underline{c}) \leq (NB)^N + B^{-1}$

(iii) $q \geq B.\ \ell(\underline{r})$

(Note that $\ell(\underline{a}) > \ell(\underline{c})$ so $\underline{a} \neq \underline{c}$).

Proof : Let $Q > 1$ be a real number. By Dirichlet's theorem there exist a rational integer t, $1 \leq t \leq Q^N$, such that

$$\left\| t \frac{a_i}{\ell(\underline{a})} \right\| \leq Q^{-1} \quad \text{for} \quad i = 1,2,\ldots,N$$

where $\underline{a} = (a_1, a_2, \ldots, a_N)$ and $\|\ \|$ denotes the distance to the nearest integer. Take $Q = NB$ and define $q = \frac{\ell(\underline{a})}{t}$. Define the vector $\underline{c} = (c_1, c_2, \ldots, c_N)$ by the conditions

$$\left\| t \frac{a_i}{\ell(\underline{a})} \right\| = \left| t \frac{a_i}{\ell(\underline{a})} - c_i \right| \quad , \quad c_i \in \mathbb{Z} \qquad \text{for } i = 1,2,\ldots,N$$

and the vector $\underline{r} = (r_1,r_2,\dots,r_N)$ by $\underline{r} = \underline{a} - q.\underline{c}$. Then (i) holds trivially. For (ii) note the inequality

$$|t - \sum_{i=1}^{N} |c_i|\,| = |\sum_{i=1}^{N} (t\frac{|a_i|}{\ell(\underline{a})} - |c_i|)| \leq \sum_{i=1}^{N} |t\frac{|a_i|}{\ell(\underline{a})} - |c_i|\,| \leq NQ^{-1} < 1.$$

Thus $t \geq 1$ implies that $\underline{c} \neq 0$. On the other hand

$$\ell(\underline{c}) = \sum_{i=1}^{N} |c_i| \leq \sum_{i=1}^{N} (|t\frac{a_i}{\ell(\underline{a})}| + Q^{-1}) \leq (NB)^N + B^{-1} .$$

Finally

$$\ell(\underline{r}) = \sum_{i=1}^{N} |a_i - q.c_i| = q \sum_{i=1}^{N} |t\frac{a_i}{\ell(\underline{a})} - c_i| \leq qB^{-1}$$

which proves (iii).

<u>Proof of Theorem 1</u> : Let $F(z) = \sum_{i=1}^{k} a_i z^{n_i} \in \mathbb{Z}[z]$. If the exponents $n_1,n_2,\dots,n_k$ are fixed, then, with each vector $\underline{a} = (a_1,a_2,\dots,a_k)$, we can associate the polynomial $a(z) = \sum_i a_i z^{n_i}$ and conversely. If $\ell(F) \leq (k+1)^k$ then the assertion of the theorem holds by Lemma 2. Otherwise, let $\underline{F} \in \mathbb{Z}^k$ be the vector corresponding to F. Then

$$\ell(\underline{F}) = \ell(F) > kB^k + 1 \qquad \text{with} \qquad B \geq 1 + \frac{\log 2e}{2e}\,\frac{1}{(k+1)^k} .$$

By Lemma 3 $\underline{F} = \underline{r} + q.\underline{c}$ with $\underline{r} \in \mathbb{Q}^k$ and $\underline{c} \in \mathbb{Z}^k$. Further $q \geq B$. $\ell(\underline{r})$ and $\underline{F} \neq \underline{c}$. If F,r,c are the corresponding polynomials then $F \neq c$ implies that $r \neq 0$ and $(F,c) = 1$ because of the irreducibility of F. Hence

$$\prod_{F(\alpha)=0} r(\alpha) = \prod_{F(\alpha)=0} (-q.c(\alpha))$$

and

$$\ell(r)^{|F|}M(F)^{|F|} \geqslant q^{|F|}$$

So $M(F) \geqslant B$.

Proof of Corollary 1 : Assume that $\ell(F) > k^k + 1$. Then $\ell(F) > kB^k + 1$ with some $B > 1$ and, by Lemma 3, $F = r + q.c$ with $c(z) \in \mathbb{Z}[z]$ and $q \geqslant B\,\ell(r)$. Further $\ell(c) < \ell(F)$ and $|c| \leqslant |F|$. So F does not divide c and there exists a cyclotomic polynomial f dividing F and not dividing c. Hence

$$0 \neq \prod_{f(\alpha)=0} r(\alpha) = \prod_{f(\alpha)=0} (-q.c(\alpha))$$

and

$$\ell(r)^{|f|}M(f)^{|F|} \geqslant q^{|f|}$$

which gives the contradiction $1 = M(f) \geqslant B > 1$.

References

[1] P. E. Blanksby and H. L. Montgomery, Algebraic integers near the unit circle Acta Arith. 28 (1971), pp.355-369.

[2] E. Dobrowolski , On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. 34 (1979), pp.125-135.

[3] E. Dobrowolski, W. Lawton, A. Schinzel, On a problem of Lehmer, Acta Math. Acad. Sci. Hungaricae (to appear).

[4] W. Lawton, Asymptotic properties of roots of polynomials-preliminary report, Proceedings of the Seventh Iranian National Mathematical Conference, Azarabadegan University, Tabris, Iran, March 1976.

[5] D. H. Lehmer, Factorization of certain cyclotomic functions, Ann. Math. 2, 34 (1933), pp.461-479.

[6] C. L. Stewart, On a theorem of Kronecker and related question of Lehmer, Séminaire de théorie des nombres, Bordeaux , 1977-78, n°7, 11p.

Wrocław University
Institute of Mathematics
Pl. Grunwaldski 2/4
50-384 Wrocław (Poland)

YUVAL Z. FLICKER

Linear forms on arithmetic abelian varieties : ineffective bounds

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 41-47

<http://www.numdam.org/item?id=MSMF_1980_2_2__41_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 41-47

LINEAR FORMS ON ARITHMETIC ABELIAN VARIETIES : INEFFECTIVE BOUNDS

by

Yuval Z. FLICKER

Using ideas from Baker's method of linear forms in logarithms, Masser, Lang and Coates gave effective lower bounds for linear forms in algebraic points on an abelian variety of CM-type. In [1,3] it was shown that analogous effective bounds hold for the p-adic valuations of such forms for a certain class of primes p (depending on the ring of complex multiplications ; see [1,3]). It would be of interest to obtain such bounds for all abelian varieties, not only of CM-type, and in the p-adic case for all primes unconditionally ; however no-one has yet succeeded in doing this. Confining ourselves to non-effective lower bounds we shall here obtain such bounds for any "arithmetic" abelian variety and all valuations. The first result of the kind which we shall establish was given by Gelfond as a consequence of the Thue-Siegel theory ; hence the ineffective character of the proof. Coates [2] obtained an analogue in the complex elliptic case, applying methods similar to those used by Siegel [7] in the study of integral points on curves of genus 1. Theorem 1 below will depend on the general Thue-Siegel-Mahler-Roth theorem.

Theorem 2 is a geometric reformulation of Theorem 1 ; thus we find a lower bound for the (complex or p-adic) Euclidean distance of a variable point P with algebraic components from a fixed point on the abelian variety, in terms of the height H(P) of the point P. Such reformulation is implicit in Siegel [7] , was made explicit by Lang [4] and later by Masser [5] (see [1,3] for the p-adic case).

This will be applied to deduce a slight improvement of the Siegel(-Mahler) theorem on the finiteness of the number of points on a curve of positive genus which lie in fixed number field K and whose denominator is composed of primes from a finite set. The present variant of the proof of the Siegel-Mahler theorem seems to emphasize more clearly the underlying Diophantine connections.

Applications improving the Siegel-Mahler theorem can be deduced in the same way also from the effective lower bounds for linear forms which can be obtained using the Baker-Masser approach. We note that the sharper but specialized results of [6] and [3] imply a very sharp version of the above theorem in the case of CM-type curves, when the denominator is composed of a special kind of primes. Even in this last case the result is ineffective since we use a base for the K-rational points on A which is given ineffectively by the Mordell-Weil theorem.

§ 1. Let A be an abelian variety with dimension d in a projective space of dimension $d'(\geq d)$. Let K be a number field, and suppose that A, its group law, and its origin e are defined over K. Signify by $\{X_o, X_1, \ldots, X_{d'}\}$ a set of projective coordinates for A, such that $X_o(e) \neq 0$ and $X_i(e) = 0 (1 \leq i \leq d')$; we can always find such set by applying a projective linear transformation. Then $\{x_i = X_i/X_o\}$ is a set of affine coordinates for the affine open subset A_o of the points P on A with $X_o(P) \neq 0$. We shall consider first the points on A_o which are defined over the field of complex numbers, and later the points which are defined over a p-adic completion $K_{\mathfrak{p}}$ of K.

In the complex case we recall that there is a lattice L in $\mathbb{C}^d$, and a locally injective map $\underline{f} = (f_1, \ldots, f_{d'})$, whose d' components are analytic functions on an open subset of $\mathbb{C}^d$ with periods in L, which parametrizes A_o, and such that $f_i(\underline{O}) = 0 (1 \leq i \leq d')$. Moreover $\underline{f}$ is a local analytic isomorphism at each point in its domain of convergence, and it can be continued as a meromorphic map to the entire space.

In the p-adic case we also have a parametrization of a neighborhood of e on A_o by an injective map $\underline{f} = (f_1, \ldots, f_{d'})$, with d' analytic components, and such that $f_i(\underline{O}) = 0 (1 \leq i \leq d')$; however it is no longer periodic but only locally defined on the neighborhood $|\underline{z}| < p^{-1/(p-1)}$ of the origin in $K_{\mathfrak{p}}^d$. Moreover we may assume that $\underline{f}$ is an isometry in the p-adic case, see [1], but this will not be needed here. In both cases we say that a vector $\underline{u}$ in $\mathbb{C}^d$ or in $K_{\mathfrak{p}}^d$, at which $\underline{f}$ converges, is an <u>algebraic point</u>, if each f_i takes an algebraic value at $\underline{u}$.

Now suppose that $\underline{u}_1,\ldots,\underline{u}_m$ are algebraic points which are linearly independent over $\mathbb{Q}$. Since we shall deal simultaneously both with the complex and with the p-adic cases, we shall signify by $|\ \ |$ any valuation on K. We prove :

Theorem 1 : *For any* $\varepsilon > 0$ *there exists a constant* $C > 0$, *such that for any set of integers* $b_1,\ldots,b_m$, *not all* 0, *with absolute values at most* B, *we have*

$$|b_1\underline{u}_1 + \ldots + b_m\underline{u}_m| > C \exp(-\varepsilon B^2).$$

The constant C depends on ε, $f_i(\underline{u}_j)\,(1 \leqslant i \leqslant d',\ 1 \leqslant j \leqslant m)$, the defining equations of A and on the valuation $|\ \ |$. As we already remarked C cannot be explicitly computed in these terms, but it will be, once an effective analogue of the Thue-Siegel-Mahler-Roth theorem is established .

§ 2. We shall now proceed to prove Theorem 1 both in the complex and in the p-adic cases. In both cases we shall prove the theorem by deducing a contradiction from the supposition that there are infinitely many sets of integers $b_1,\ldots,b_m$ such that $u = b_1\underline{u}_1 + \ldots + b_m\underline{u}_m$ does not satisfy the conclusion of Theorem 1. Assuming this, we let n be a natural number, whose value will be specified later, such that the greatest common divisor (p,n) of p and n is 1 in the p-adic case. We write $b_i = nb_i' + q_i$, where b_i' and q_i are rational integers and $0 \leqslant q_i < n$; thus $\underline{u} = n\underline{u}' + \underline{q}$, where

$$\underline{u}' = b_1'\underline{u}_1 + \ldots + b_m'\underline{u}_m \text{ , and } \underline{q} = q_1\underline{u}_1 + \ldots + q_m\underline{u}_m \ .$$

Clearly $\underline{q}$ can take only a finite number of values when n is fixed ; we will restrict our attention in the sequel to a fixed $\underline{q}$ ($= \underline{q}(n)$), and to an infinite sequence of distinct sets $b_1',\ldots,b_m'$, corresponding to $\underline{q}$. On denoting by B' the maximum of the absolute values of $b_i'\,(1 \leqslant i \leqslant m)$, we have $B \geqslant \frac{1}{2}nB'$, provided that $B' \geqslant 2$. In the sequel the constants implied by $\ll$ will signify positive numbers which are effectively computable in terms of ε ,n, $f_i(\underline{u}_j)$, the defining equations of A, and the valuation $|\ \ |$. For the validity of the subsequent arguments, we may assume that $B' \gg 1$. Since $|\underline{u}| < e^{-\varepsilon B^2}$ and $(p,n) = 1$ in the p-adic case, we have

$$|\underline{u}' + \underline{q}/n| < e^{-\frac{1}{4}\varepsilon n^2 B'^2} \tag{1}$$

We claim that without loss of generality $\underline{f}$ converges at a sufficiently small (but independent of n) neighborhood of $-\underline{q}/n$. This is easy to show in the p-adic case, since by assumption f converges at $\underline{u}_1,\ldots,\underline{u}_m$, we have $(p,n) = 1$, and $q_1,\dots,q_m$ are rational integers ; thus $|q_i/n| < 1$ in the p-adic valuation, and it follows that $-\underline{q}/n$ belongs to the domain of convergence of $\underline{f}$. In the complex case we argue similarly . Since $\underline{f}$ is analytic at a sufficiently small neighborhood of $\underline{O}$, and since $|q_i/n| < 1$, it suffices to show that for each i the number $|\underline{u}_i|$ is small enough. But this can be assumed without loss of generality, upon replacing $\underline{u}_i$, by $\underline{u}_i/k$, where k is a sufficiently large fixed integer ; note that $\underline{u}_i/k$ are again algebraic points, since the group law on A is defined over K; observing that near $-\underline{q}/n$ the map $\underline{f}$ is an analytic isomorphism, we deduce from (1) that

$$|\underline{f}(\underline{u}') - \underline{f}(-\underline{q}/n)| < e^{-(\varepsilon/5)n^2B'^2} \; ; \tag{2}$$

also we conclude that there is some $i(1 \leq i \leq d')$ such that $f_i(\underline{u}')$ are distinct for infinitely many $\underline{u}'$.

The height $h(a) = h_K(a)$ of an element a of K is defined to be the product of $\max(1, |a|_v)^{n_v}$ over all valuations $|\ |_v$ of K, where n_v denotes the degree of the completion of K at v over the corresponding completion of the rationals $\mathbb{Q}$. The height h(P) of a point $P = (1,a_1,\dots,a_{d'})$ is defined by a similar product of the terms $\max\limits_i(1,|a_i|_v)^{n_v}$. On taking a finite extension of K, if necessary, we may assume that any $f_i(\underline{u}_j)$ belongs to K. It follows from the Néron-Tate theorem that the function $\log h$ (P) of P is equal to the sum of a positive definite quadratic form, a linear form and a bounded function. Hence there is a positive constant c which depends on the $f_i(\underline{u}_j)$ and on the defining equations of A only, such that

$$\log h\,(f_i(\underline{u}')) < \log h\,(\underline{f}(\underline{u}')) < cB'^2 \; .$$

By virtue of the choice of i, (2) implies that there are infinitely many $\underline{u}'$ with distinct $f_i(\underline{u}')$, such that

$$|f_i(\underline{u}') - f_i(-\underline{q}/n)| < h(f_i(\underline{u}'))^{-\varepsilon' n^2} \tag{3}$$

where $\varepsilon' = \varepsilon/6c$. We note that for any $\underline{u}'$ the number $f_i(\underline{u}')$ lies in K, since the group law of A is defined over K, and the $f_i(\underline{u}_j)$ belong to K . Similarly, since $f_i(-\underline{q}/n)$ is a component of an nth division point of $\underline{f}(-\underline{q})$, we deduce that $f_i(-\underline{q}/n)$ is algebraic. But as soon as n is so large that $\varepsilon' n^2 > 2$, the inequality (3) contradicts the conclusion of the Thue-Siegel-Mahler-Roth theorem, and the proof is complete.

In the case that A is an abelian variety of CM-type, namely, when the tensor product $k = \mathrm{End}\, A \otimes \mathbb{Q}$, of the ring End A of endomorphisms of A and the rationals $\mathbb{Q}$, has a structure of a quadratic imaginary extension of a totally real field k_1 with $[k_1 : \mathbb{Q}] = d$, a much stronger but specialized result is known. It says that for any archimedean or p-adic valuation of K, where the rational prime p splits completely in k_1 and all of its k-prime divisors have the same splitting type, we have :

Theorem 1' : *For any* $\varepsilon > 0$ *there exists a positive constant* C', *effectively computable in terms of* ε, A, $|\ |$, *and* $f_i(\underline{u}_j)$, *such that for any set of integers* $b_1,\dots,b_m$, *not all* 0, *with absolute values at most* B, *we have*

$$|b_1\underline{u}_1+\dots+ b_m\underline{u}_m| > C' \exp\{-(\log B)(\log \log B)^{1+dm+\varepsilon}\}.$$

Proof : This is proved in [6] in the archimedean case, and [3] in the non-archimedean case.

In fact the results of [6] and [3] are more general, and Theorem 1' is established there with coefficients b_i which are arbitrary diagonal matrices, not all singular, with algebraic entries. However for the applications that we have in mind it suffices to use only the statement given above.

§ 3. Theorems 1 and 1' have the following geometric reformulations. Let d(e,P) denote the Euclidean distance either in the space $\mathbb{C}^{d'}$ or in the space $K^{d'}$ between the origin e and an arbitrary point P on A_o. We have :

Theorem 2 : *For any* $\varepsilon > 0$ *there exists a positive constant* C_1 *such that for any point* $P(\neq e)$ *on* A_o *with coordinates in* K *we have*

$$d(e,P) > C_1\, h(P)^{-\varepsilon} .$$

When A is of CM-type and $|\ |$ satisfies the splitting assumption of theorem 1', we have :

Theorem 2' : For any $\varepsilon > 0$ there exists a positive constant C_1' , such that for any point $P(\neq e)$ on A_o with coordinates in K we have

$$d(e,P) > C_1'(\log h(P))^{-(\log\log\log h(P))^{1+dr+\varepsilon}}$$

where r denotes the rank of the Mordell-Weil group A_K.

The constants C_1 and C_1' depend on the (ineffective) determination of a base for the Mordell-Weil group A_K of K-rational points on A, in addition to the parameters on which the constants C and C' (of Theorems 1 and 1') depend (in particular, they depend on the given valuation).

The deduction of Theorem 2 (resp. 2') from Theorem 1 (resp. 1') which is similar to the discussion in [5] , was written out in chapter IV, section 3, of the author's 1978 Cambridge UK thesis, and there is no need to repeat the details here. This comment also applies to the deduction of Theorem 3 (resp. 3') below from Theorem 2 (resp. 2').

Finally the above results can be applied to investigate K-rational points on algebraic curves of positive genus. Thus we consider an affine algebraic plane curve E (of positive genus) such that there exists a non-constant rational map $b : E \to A$, where A is an abelian variety, and E, b and A are defined over K. Let V be a finite set of valuations on K including all of the infinite primes. We define the (generalized) size $S_V(P)$ of a K-rational point $P = (x,y)$ on E to be the product of the terms $M_v = \mathrm{Max}(1, |X|_v, |y|_v)^{n_v}$ over all primes v in V ; similarly we define the (generalized) denominator $D_V(P)$ of P to be the product over all primes v outside V of the terms M_v. We have :

Theorem 3 : For any $\varepsilon > 0$ there exists a positive constant C_2, such that for any K-rational point P on E we have

$$S_V(P) < C_2 D_V(P)^{\varepsilon}$$

The Siegel-Mahler theorem asserts that the number of K-rational points on E whose denominators consist of powers of primes from a finite set W of K-primes is finite. This can be deduced from Theorem 3 on taking A to be the Jacobian variety of the curve and a set V of valuations on K which contains W, and on putting $D_V(P) = 1$.

If A is of CM-type with dimension d and V is a finite set of valuations on K, which in addition to all archimedean valuations, contains only valuations for which Theorems 1' and 2' hold, we have :

Theorem 3' : For any $\varepsilon (0 < \varepsilon < 1)$ there exists a positive constant C_2' such that for any K-rational P on E we have

$$S_V(P) < C_2'(\log D_V(P))^{(\log \log \log D_V(P))^{1+dr+\varepsilon}}$$

The constants C_2 and C_2' depend on ε, V, K and E, and are as ineffective as the constants C_1 and C_1' (respectively).

References

[1] Bertrand D., and Flicker, Y., Linear forms on abelian varieties over local fields, Acta Arith., to appear.

[2] Coates, J. , An application of the Thue-Siegel-Roth theorem to elliptic functions, Proc. Camb. Phil. Soc., 69 (1971) 157-61.

[3] Flicker, Y. , Linear forms on abelian varieties over local fields : a sharpening, preprint.

[4] Lang, S., Diophantine approximations on toruses, Amer. J. Math., 86 (1964), 521-33.

[5] Masser, D.,Linear forms in algebraic points of abelian functions III, Proc. London Math. Soc., 33 (1976), 549-64.

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

[7] Siegel, C. , Über einige Anwendungen Diophantischer Approximationen, Abh. Preuss. Akad. Wiss., 1 (1929) ; Ges. Ab. I., 242-66.

Department of Mathematics
Columbia University
New York, New York 10027
U. S. A.

MÉMOIRES DE LA S. M. F.

BENEDICT H. GROSS
DON ZAGIER

On the critical values of Hecke L-series

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 49-54
<http://www.numdam.org/item?id=MSMF_1980_2_2__49_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 49-54

ON THE CRITICAL VALUES OF HECKE L-SERIES

by

Benedict H. GROSS

and

Don ZAGIER

Let E be the elliptic curve over $\mathbb{Q}$ with minimal model

$$y^2 + xy = x^3 - x^2 - 2x - 1 \quad .$$

The modular invariant, discriminant, and conductor of E are given by

$$j = -3^3 \, . \, 5^3$$

$$\Delta = -7^3$$

$$N = (7^2) \quad .$$

Let Ω denote the fundamental real period of the Néron differential $\omega = \frac{dx}{2y+x}$ on E :

$$\Omega = \int_{E(\mathbb{R})} \omega = 1.93331170561681...$$

Over the field $K = \mathbb{Q}(\sqrt{-7})$, E has complex multiplication by $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Hence Ω can be determined explicitly, using an identity of Chowla and Selberg [1] :

$$\Omega = \frac{\Gamma(1/7)\Gamma(2/7)\Gamma(4/7)}{\sqrt{-7}\ .\ 2\pi i} .$$

Similarly, the L-series of E is equal to the L-series of a Hecke character χ of K. The conductor of χ is the ideal $(\sqrt{-7})$; for $\mathfrak{a}$ an ideal of K which is prime to 7 :

$$\chi(\mathfrak{a}) = \alpha \quad \text{where} \quad \mathfrak{a} = (\alpha) \ , \ \alpha^3 \equiv 1 (\text{mod} \sqrt{-7})$$

We have calculated the central critical values of the Hecke L-series which are associated to odd powers of the character χ. Let $n \geq 1$ be an integer ; the Dirichlet series

$$L(\chi^{2n-1},s) = \Sigma \frac{\chi^{2n-1}(\mathfrak{a})}{\mathbb{N}\mathfrak{a}^s}$$

converges absolutely in the right half-plane $\mathrm{Re}(s) > n + \frac{1}{2}$. It extends to a holomorphic function on the entire complex plane : the modified function $\Lambda(\chi^{2n-1},s) = (7/2\pi)^s\ \Gamma(s)\ L(\chi^{2n-1},s)$ satisfies Hecke's functional equation :

$$\Lambda(\chi^{2n-1},s) = (-1)^{n+1}\ \Lambda(\chi^{2n-1},2n-s) .$$

It follows that the value of $L(\chi^{2n-1},s)$ at $s = n$, the center of the critical strip, vanishes when n is even.

When n is odd, define a_n by

$$L(\chi^{2n-1},n) = \frac{\Omega^{2n-1}}{(2\pi i/\sqrt{-7})^{n-1}} \frac{a_n}{(n-1)!} .$$

(We found this normalization by trial and error ; it is consistent with the work of Katz on the interpolation of real analytic Eisenstein series [2].)

The values of a_n for $1 \leq n \leq 33$ are listed in Table 1.

Table 1

n	a_n
1	$1/2$
3	2
5	2
7	$2(3)^2$
9	$2(7)^2$
11	$2(3^2.5.7)^2$
13	$2(3.7.29)^2$
15	$2(3.7.103)^2$
17	$2(3.5.7.607)^2$
19	$2(3^3.7.4793)^2$
21	$2(3^2.5.7.29.2399)^2$
23	$2(3^3.5.7^2.10091)^2$
25	$2(3^2.7^2.29.61717)^2$
27	$2(3^2.5^2.7^2.13.53^2.79)^2$
29	$2(3^4.5^2.7^2.113.127033)^2$
31	$2(3^5.5.7^2.71.1690651)^2$
33	$2(3^4.5.7^2.1291.1747169)^2$

Let $p \equiv 1 (\text{mod } 4)$ be a prime and let χ_p be the Hecke character

$$\chi_p(\mathfrak{a}) = \left(\frac{\mathbb{N}\mathfrak{a}}{p}\right) \chi(\mathfrak{a}) \ .$$

The Hecke L-series $L(\chi_p,s)$ is equal to the L-series of an elliptic curve $E_p/\mathbb{Q}$ which becomes isomorphic to E over $\mathbb{Q}(\sqrt{p})$. Let $\Omega_p = \Omega/\sqrt{p}$ and define $a_n^{(p)}$ by

$$L(\chi_p^{2n-1},n) = \frac{\Omega_p^{2n-1}}{(2\pi i/\sqrt{-7})^{n-1}}\,\frac{a_n^{(p)}}{(n-1)!}\ .$$

Again, $a_n^{(p)}$ vanishes when n is even. For n odd and $p = 5, 13, 17, 29, 53$ we found the values listed in Table 2.

Table 2

n \ p	5	13	17	29	53
1	1	1	1	2	0 [rank $E_{53}(\underline{Q}) = 2$]
3	$(2^2)^2$	$(2^2 . 3)^2$	$(2 . 3 . 13)^2$	$2(2^2 . 3)^2$	$2(2^3 . 7)^2$
5	$(2^2 . 5)^2$	$(2^2 . 157)^2$	$(2 . 271)^2$	$2(2^2 . 5 . 37)^2$	$2(2^4 .3.5^2 .7)^2$
7	$(2^2 .3.5.61)^2$	$(2^2 .3^2 .1847)^2$	$(2.3^2 .61)^2$	$2(2^2 .3^2 .11.29.61)^2$	$2(2^3 .3.5^2 .7^2 .13.17)^2$
9	$(2^2 .5.7.199)^2$	$(2^2 .7.13.5813)^2$	$(2.7.266977)^2$	$2(2^2 .7.17.80779)^2$	$2(2^5 .3.7^2 .19.2699)^2$
11	$(2^2 .5^2 .271)^2$	$(2^2 .3^3 .5.7.13.1021)^2$	$(2.3^4 .5.7.17.2081)^2$	$2(2^2 .3^3 .5^3 .7.13.29.79)^2$	$2(2^3 .3^2 .5^2 .7^2 .11.129893)^2$
13	$(2^2 .3.5^2 .7.3767)^2$	$(2^2 .3.7.13.3747629)^2$			
15	$(2^2 .3.5^2 .7.89.13687)^2$	$(2^2 .3^2 .7.13.101.317.15307)^2$			
17	$(2^2 .3.5^4 .7.26737)^2$	$(2^2 .3.5.7.13.4877.6510011)^2$			

Note : In all the cases we computed, $a_n^{(p)}$ is either a square or twice a square, depending on whether $(\frac{p}{7})$ is -1 or +1 . Can one prove this is general ? Are there "higher Tate-Shafarevitch groups" associated to the abelian varieties $(E_p)^{2n-1}$ whose orders can be conjecturally related to $a_n^{(p)}$? Do these groups carry a natural alternating pairing ?

Bibliography :

[1] CHOWLA S., and SELBERG A., On Epstein's Zeta Function. J. Crelle 227 (1967), 96-110.

[2] KATZ N., p-adic interpolation of real analytic Eisenstein series. Annals Math. 104 (1976), 459-571.

B. Gross
Princeton University
Fine Hall
Princeton, N. J. 08540 (U.S.A.)

D. Zagier
Mat. Inst. d. Univ. Bonn
Wegelerstrasse 10
53 Bonn (B.R.D.)

MÉMOIRES DE LA S. M. F.

D. W. MASSER

On quasi-periods of abelian functions with complex multiplication

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 55-68

<http://www.numdam.org/item?id=MSMF_1980_2_2__55_0>

SOCIÉTE 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 $\underline{\omega}$ 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].

Lemma 1 : Let ℓ be sufficiently large. Then F_ℓ contains M_ℓ .

Proof : 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 $f_1(\underline{z}_1),\ldots,f_n(\underline{z}_1)$ and $f_1(\underline{z}_2),\ldots,f_n(\underline{z}_2)$. 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

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

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])

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

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>

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

<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 $\pmod{\mathfrak{p}}$ 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 $\pmod{\mathfrak{p}}$ for the quadruple (s_1, s_2, s_3, s_4), and therefore at most 4 possibilities $\pmod{\ell}$. 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

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

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, $c_2,\dots$ denote positive constants independent of k.

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

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

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

Proof : 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 $Q(X_1,\dots,X_q)$ 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 $\beta_1,\dots,\beta_q$ put $\gamma = Q(\beta_1,\dots,\beta_q)$. Then by estimating separately at each valuation we obtain

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

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

Proof : Analyticity follows as on p.247 of [5], since $\chi(\underline{O}) \neq O$. 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 $f_1(\underline{z}),\dots,f_n(\underline{z})$ with coefficients in F. If $m = 2^{\ell-1} - 1$, the proof of Lemma 3.5 of [5] shows that

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

where

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

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

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

and so lies in F_ℓ. Again we have $H(\beta_i) \leqslant c_4^\ell$ $(O \leqslant i \leqslant \ell - 2)$ and so from (13) with $q = \ell$ we deduce $H(m\ell\varepsilon) \leqslant c_5^\ell s$. 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 $O \leqslant i \leqslant C$, let $\ell \leqslant S^{i/8}$ be a sufficiently large prime which does not split in K_O, and for positive integers $r < \ell$ and $s \leqslant S^{1+(i/4)}$ 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 $i \leqslant C$ 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

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

for some t as in the lemma. Since the rational primes which do not split in K_O 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

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

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

$$\log H(\xi) < c_9k\log k + c_9k(\ell + \log s) < c_{10}ks^{1/8}.$$

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

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

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

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

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 $F\,[f_1(\underline{z}),\dots,f_n(\underline{z})]$ 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

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

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 $\underline{\sigma}\underline{\omega}/\ell$. 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 $\underline{\sigma}\underline{\omega}/\ell$ 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

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

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

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

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

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

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 $m \leqslant 12$ 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 $0 \leqslant r < \ell$, 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 $N_r \leqslant 2(4m)^4$ 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)

YU. V. NESTERENKO

Sur une méthode d'élimination et ses applications à la théorie des nombres transcendants

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 69

<http://www.numdam.org/item?id=MSMF_1980_2_2__69_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 69

SUR UNE MÉTHODE D'ÉLIMINATION ET SES APPLICATIONS A LA THÉORIE DES NOMBRES TRANSCENDANTS

par Yu. V. Nesterenko

Soient f_1 et f_2 deux fonctions analytiques au voisinage du point $z=0$, algébriquement indépendantes sur $\mathbb{C}(z)$, et vérifiant le système différentiel

$$y_i' = q_{io} + q_{i1}y_1 + q_{i2}y_2 \quad (i=1,2),$$

où les q_{ij} sont des éléments de $\mathbb{C}(z)$. Alors, il existe une constante $C = C(f_1,f_2)$, telle que, pour tout polynôme $P \in \mathbb{C}[Z,X_1,X_2]$, $P \not\equiv 0$, l'inégalité suivante soit satisfaite :

$$\mathrm{ord}_{z=o} P(z,f_1(z),f_2(z)) \leq C(\deg_Z P+1)(\deg_X P)^2 .$$

[Cet énoncé précise un résultat général de l'auteur paru aux Math.U.S.S.R. Izvestija, vol.11, 1977, n°2, pp.239-270].

Université d'Etat de Moscou
Département de Mathématiques
Moscou 117234
(U.R.S.S.)

ALF VAN DER POORTEN

Linear forms in logarithms, effectivity and elliptic curves

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 71

<http://www.numdam.org/item?id=MSMF_1980_2_2__71_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 71

LINEAR FORMS IN LOGARITHMS, EFFECTIVITY AND ELLIPTIC CURVES.

by Alf van der Poorten

It is well known that effectively computable lower bounds for linear forms in logarithms, in both the complex and p-adic cases, provide an effective method for computing all integer points on an elliptic curve (or, for that matter, on appropriate curves of higher genus). In particular, since elliptic curves,of given conductor give rise to integer points on (other) elliptic curves one may effectively compute all elliptic curves over $\mathbb{Q}$ of given conductor. What is not so well known is that these effective methods have been rendered quite practical by a combination of improved computer technology and by a sharpening of the lower bounds for linear forms in logarithms. Where once the concept "Baker bound" was synonymous with "absurdly large, but finite,number" the bounds that we now obtain in Baker's method may be quite reasonable numbers of order 10^{10} or so. We will discuss these matters and related computations concerning elliptic curves over $\mathbb{Q}$.

Macquarie University
School of Mathematics
North Ryde
NSW 2113
(Australia)

MÉMOIRES DE LA S. M. F.

M. J. RAZAR

Some functions related to the derivatives of the L-series of an elliptic curve at s=1

Mémoires de la S. M. F. 2^{e} série, tome 2 (1980), p. 73-74

<http://www.numdam.org/item?id=MSMF_1980_2_2__73_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 73-74

SOME FUNCTIONS RELATED TO THE DERIVATIVES OF THE L-SERIES OF AN ELLIPTIC CURVE AT $s = 1$.

by M. J. Razar

If E is an elliptic curve defined over the rationals and having complex multiplication then it is well known that its L-series may be identified with a Hecke L-series with Grössencharakter. In their paper [1], Birch and Swinnerton-Dyer state the beautiful conjecture which now bears their names concerning the relationship between the arithmetic of the curve and the initial term in the Taylor expansion of $L_E(s)$ about $s = 1$. Their paper gives extensive evidence for the correct value of $L_E(1)$ in the above named case.

Further evidence (e.g. [4], [5], [7]) has accumulated over the years but certainly the most striking work is due to Coates and Wiles [2] who prove that if the group of rational points $E(\mathbb{Q})$ is infinite then $L_E(1) = 0$. Moreover, they give considerable insight into the (p-adic) correctness of the Birch-Swinnerton-Dyer predictions when $L_E(1) \neq 0$.

Considerably less is known about the first term in the expansion of $L_E(s)$ about $s = 1$ when $L_E(1) = 0$. Stephens ([7]) provides some numerical evidence. Birch (unpublished, to the best of my knowledge) has given a rather precise prediction in the rank 1 case ($L_E'(1) \neq 0$), by expressing the canonical height in terms of the Weierstrass sigma function.

One of the major obstacles in the study of $L_E(s)$ when $L_E(1) = 0$ has been the lack of suitable formulas for proving algebraicity and p-adic results about, say, $L_E'(1)$. In my talk I propose to discuss a close relation existing between the 'higher terms" of Kronecker's limit formulas (e.g. the Laurent expansion of $\Sigma\Sigma\, |mz + n|^{-2s}$ about $s = 0$ or $s = 1$) and the expansion of $L_E(s)$. Not surprisingly some of the functions arising in this context are explicable in terms of Bessel functions -but in a case where they simplify substantially. In addition, we are led to introduce some non meromorphic elliptic functions.

There are some analogies and connection between the above mentioned functions and the functions associated to the full Taylor expansions of Hurwitz-type zeta functions at non positive integers. In the latter situation some rather precise rationality statements can be proved. Koblitz and Ogus and, independently, Kubert have proved one such result in a slightly different formulation and I believe Gross will be discussing the p-adic significance of some of these ideas. For a fairly general "rationality" statement concerning the first non zero coefficient in the expansion of certain linear combinations of Dirichlet L-functions at non positive integers, see [6].

REFERENCES

[1] B. J. Birch and H.P.F. Swinnerton-Dyer : Notes on elliptic curves II, J. Reine u.angew. Math. vol. 218 (1965) pp.79-108.

[2] J. Coates and A. Wiles : On the conjecture of Birch and Swinnerton-Dyer, Inventiones Math. 39 (1977), pp.223-253.

[3] D. Goldfeld : The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer, Annali Scuola Normale Superiore.

[4] M. J. Razar : The non vanishing of L(1) for certain elliptic curves, American Journal of Math., 96 (1974), pp.104-126.

[5] M. J. Razar : A relation between the two component of the Tate-Safarevic group and L(1) for certain elliptic curves, American Journal of Math. 96 (1974), pp.127-144.

[6] M. J. Razar : The value of the first non vanishing derivative at non positive integers of linear combinations of Dirichlet L-series (preliminary draft).

[7] N. Stephens : The conjectures of Birch and Swinnerton-Dyer about $X^3 + Y^3 = DZ^3$.

[8] A. Weil : Elliptic functions according to Eisenstein and Kronecker Springer Verlag, New York, 1976.

The University of Maryland
Department of Mathematics
College Park , Maryland 20742
(U. S. A.)

MÉMOIRES DE LA S. M. F.

K. A. RIBET

Division fields of abelian varieties with complex multiplication

Mémoires de la S. M. F. 2^e série, tome 2 (1980), p. 75-94

<http://www.numdam.org/item?id=MSMF_1980_2_2__75_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 75-94

DIVISION FIELDS OF ABELIAN VARIETIES WITH COMPLEX MULTIPLICATION

by

K. A. RIBET

1. Let A be an abelian variety over a number field k. Suppose that A has complex multiplication over k in the sense that $(\mathrm{End}_k A) \otimes \mathbb{Q}$ contains a commutative semisimple algebra E over $\mathbb{Q}$ of rank 2.dim A. For $N \geqslant 1$, let d(N) be the dègree over k of the field $k(A_N)$ obtained by adjoining to k the kernel A_N of multiplication by N on A. Let $\alpha(N)$ be the number of (distinct) prime factors of N. The main purpose of this paper is to prove the following result :

THEOREM (1.1) : *There exist positive constants* C_1, C_2 *and an integer* $\nu \geqslant 0$ *(depending on A, k, and E) such that we have*

$$C_1^{\alpha(N)} < \frac{d(N)}{N^{\nu}} < C_2^{\alpha(N)}$$

for all $N \geqslant 1$.

We prove (1.1) by writing the ℓ-adic representations of A in the form given them by Serre-Tate [15] (using the theory of Shimura-Taniyama [17] and Weil [18]) and then exploiting some elementary facts about the "mod ℓ^n" points of tori over $\mathbb{Q}$. The possibility of doing this was suggested by a letter from Serre to Masser [13] concerning the special case where A is a product of several elliptic curves*; to prove (1.1) we have followed Serre's arguments. It should be noted that a variant of (1.1) was proved by T. Kubota [4], who considered integers N of the form ℓ^n, ℓ being a fixed prime. Also, in this volume, Masser [6] has treated prime numbers N, for abelian varieties of dimension 2.

In our proof of (1.1), the integer ν arises as the dimension of a certain torus which is familiar in other contexts. Namely, it is the Hodge group of A (see [1] and §§ 3,4 of [14]), and so its dimension bounds the transcendence degree of the field generated by the periods of differentials on A [1]. For us, the torus is given as the image of a certain explicit map between tori ; therefore, via the dictionary between tori and their character groups, computing ν comes down to computing the rank of a certain matrix. In § 3 of this paper, we write down explicitly the matrix that intervenes, and this enables us to give the lower bound $2+\mathrm{Log}_2 d$ for ν in the case where A is absolutely simple, d denoting the dimension of A. There is also a trivial upper bound for ν, namely the sum of 1 and the dimension of A. When ν attains this upper bound, we say (following Kubota) that A is "non-degenerate." For A absolutely simple, it follows from our lower bound that A is always non-degenerate for d = 1,2,3. We give several examples (due, variously, to Shimura, Serre, and Lenstra) of absolutely simple A which do not have this property. The smallest example has d = 4 and $\nu = 4$; this is given by the CM type constructed by Mumford and described in [9].

For the reader who was present at the Conference, it might be pointed out that this article bears no relation to the author's talk, for which one can consult [10]. The material concerning the calculation of ν is based on a manuscript written in 1977-78 after correspondence with Masser and discussions with Serre and Lenstra. It later formed the basis for a talk by the author at the Rennes conference on algebraic geometry in June, 1978.

* For the convenience of the reader, the text of this letter (and a sequel) has been included as an appendix to this paper.

2. Let T be a torus over $\mathbb{Q}_\ell$, and let

$$X(T) = \mathrm{Hom}_{\overline{\mathbb{Q}}_\ell}(T, \mathbb{G}_m)$$

be the character group of T. Using an idea of Ono [7,§ 2], we define subgroups $T(1+\ell^n\mathbb{Z}_\ell)$ $(n > 0)$ of $T(\mathbb{Q}_\ell)$ by the rule

$$T(1+\ell^n\mathbb{Z}_\ell) = \{t \in T(\mathbb{Q}_\ell) \mid \chi(t) \equiv 1 \bmod \ell^n \text{ for all } \chi \in X(T)\} .$$

We have $\chi(t) \in \bar{\mathbb{Q}}_\ell^*$, and the condition $\chi(t) \equiv 1 \bmod \ell^n$ means that $\mathrm{ord}_\ell(\chi(t)-1)$ is at least n. Thus $T(\mathbb{Z}_\ell)$ is the maximal compact subgroup of $T(\mathbb{Q}_\ell)$, and the various $T(1+\ell^n Z_\ell)$ define a filtration of $T(\mathbb{Z}_\ell)$ by open subgroups. We further define

$$T(\mathbb{Z}/\ell^n\mathbb{Z}) = T(\mathbb{Z}_\ell)/T(1+\ell^n\mathbb{Z}_\ell) \qquad (n > 0).$$

<u>Example (2.1)</u> : Let $E = E_1 \times \ldots \times E_m$ be a product of finite extensions of $\mathbb{Q}_\ell$, and let T be the torus obtained by viewing E^* as an algebraic group over $\mathbb{Q}_\ell$. Then we have

$$T(\mathbb{Z}_\ell) = R^* ,$$

where R is the <u>integer ring</u> of E, namely the product of the integer rings of the E_i. Further, for $n > 1$ we have

$$T(1 + \ell^n\mathbb{Z}_\ell) = \{r \in R^* \mid r \in 1 + \ell^n R\} ,$$

and

$$T(\mathbb{Z}/\ell^n\mathbb{Z}) = (R/\ell^n R)^* .$$

It is easy to check that the cardinality of $T(\mathbb{Z}/\ell^n\mathbb{Z})$ is given by the formula

$$\ell^{n\nu} \cdot \prod_{i=1}^{m} \frac{q_i - 1}{q_i} ,$$

where ν is the dimension of the torus T (i.e. the sum of the degrees of the E_i over $\mathbb{Q}_\ell$) and q_i is the order of the residue field of R_i, for $i = 1,\ldots,m$. (Cf. [12], Ch.IV,§ 2, Prop. 6.) A special case occurs when E is given by $F \otimes \mathbb{Q}_\ell$, where F is a finite extension of $\mathbb{Q}$, or a product of such extensions. Then we have $T = T_{F/\mathbb{Q}_\ell}$, where T_F is the torus over $\mathbb{Q}$ defined by F^* .

Remark (2.2) : If T has "good reduction" (i.e. T is split over a finite unramified extension of $\mathbb{Q}_\ell$) , then there is a commutative smooth group scheme $T_{/\mathbb{Z}_\ell}$ whose general fibre is the torus T. One may show that $T(\mathbb{Z}/\ell^n\mathbb{Z})$ coincides with the group of $\mathbb{Z}/\ell^n\mathbb{Z}$ -valued points of $T_{/\mathbb{Z}_\ell}$, for $n > 1$. The special case $n = 1$ is particularly easy to treat because it then suffices to identify $T(\mathbb{Z}/\ell\mathbb{Z})$ with the group of rational points of the reduction $T_{/\mathbb{F}_\ell}$ of T (i.e. of $T_{/\mathbb{Z}_\ell}$)mod ℓ . For this see Prop. 2.3.1 of [7] , where $T_{/\mathbb{F}_\ell}$ is defined directly by declaring its character group to be X(T), viewed as a $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$-module (which we may do since it is an unramified $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-module by hypothesis).

We now consider a map $\lambda : T \to T'$ between $\mathbb{Q}_\ell$ -tori. For $n > 0$, it is clear that λ induces maps

$$T(1 + \ell^n\mathbb{Z}_\ell) \longrightarrow T'(1 + \ell^n\mathbb{Z}_\ell)$$

$$T(\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow T'(\mathbb{Z}/\ell^n\mathbb{Z})$$

We denote the second map by λ_n .

Theorem (2.3) : If λ is surjective, then the order of the cokernel of λ_n is bounded independently of n. If λ is an isogeny, then both the kernel and the cokernel of λ_n have bounded order.

Proof : When λ is surjective, the map

$$\alpha : T(\mathbb{Z}_\ell) \to T'(\mathbb{Z}_\ell)$$

induced by λ has an open image, as one may see by viewing the two groups as ℓ-adic Lie groups, since the surjectivity of λ just means that the map on Lie algebras induced by α is surjective. (See Bourbaki, Groupes et Algèbres de Lie, Ch. III, Prop. 28 of § 3, n° 8 and Th. 2 of § 7, n°1.) Since $T'(\mathbb{Z}_\ell)$ is compact, the cokernel of α is finite. Since the cokernel of λ_n is a quotient of this cokernel for each n, we get the first statement of the theorem.

Now assume that λ is an isogeny. Then the kernel of α is finite, and the assertion to be proved reduces, via the snake lemma, to the assertion that the cokernel of the restriction

$$\alpha_n : T(1+\ell^n\mathbb{Z}_\ell) \to T'(1+\ell^n\mathbb{Z}_\ell)$$

of α to $T(1+\ell^n\mathbb{Z}_\ell)$ has order which is bounded independently of n. For this, we consider the "transpose" isogeny $\hat{\lambda}$ and define $\hat{\alpha}_n$ for $n \geq 0$ as the map for $\hat{\lambda}$ analogous to α_n. Then $\alpha_n \circ \hat{\alpha}_n$ is just multiplication by the degree of λ on $T'(1+\ell^n\mathbb{Z})$. It is clear for n sufficiently large that $T'(1+\ell^n\mathbb{Z}_\ell)$ is isomorphic to the group $\mathbb{Z}_\ell^\nu$ where $\nu = \dim T = \dim T'$ is independent of n. Hence the cokernel of $\alpha_n \circ \hat{\alpha}_n$, and therefore that of α_n, has bounded order.

We now consider once again a surjection $\lambda : T \to T'$ over $\mathbb{Q}_\ell$, and write λ^* for the corresponding inclusion

$$X(T') \hookrightarrow X(T)$$

of character groups. Let X" be the subgroup of X(T) given by

$$X'' = \{\chi \in X(T) \mid n\chi \in \lambda^*(X(T')) \text{ for some } n \geq 1\}.$$

Then $(X'' : X(T'))$ is finite, and $X(T)/(X'')$ is torsion free. If we let T'' be the $\mathbb{Q}_\ell$ -torus corresponding to X'', then the inclusion

$$X(T') \subseteq X''$$

corresponds to an isogeny

$$\nu : T'' \to T'$$

and the inclusion $X(T'') \hookrightarrow X(T)$ corresponds to a map

$$\mu : T \to T''$$

whose kernel is connected (i.e. is a torus). We have

$$\lambda = \nu \circ \mu.$$

Theorem (2.4) : *Suppose that* $X(T)$ *is an unramified* $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell / \mathbb{Q}_\ell)$*-module, so that the tori* T, T', T'' *have good reduction. Suppose also that* ℓ *is prime to the degree* N *of the isogeny* ν . *Then, with the notation as in* (2.3), *the order of the cokernel of* λ_n *is bounded by* N. *If, furthermore,* λ *is an isogeny* (*so that* $\lambda = \nu$), *then the kernel of* λ_n *again has order bounded by* N.

Proof : It is known that the map $T(\mathbb{Z}_\ell) \longrightarrow T''(\mathbb{Z}_\ell)$ induced by μ is surjective because of the good reduction hypothesis ([8] ,§ 4.2). It will therefore be enough to prove the statements when λ is an isogeny, which we now suppose to be the case. Under our hypotheses, the map

$$\alpha_1 : T(1 + \ell\mathbb{Z}_\ell) \to T'(1 + \ell\mathbb{Z}_\ell)$$

induced by λ is known to be an isomorphism [7, Prop. 2.2.2] . It follows formally from this that the maps

$$\alpha_n : T(1 + \ell^n \mathbb{Z}_\ell) \to T'(1 + \ell^n\mathbb{Z}_\ell)$$

are isomorphisms for *all* $n \geq 1$. [Given $t' \in T'(1+\ell^n\mathbb{Z}_\ell)$, suppose that $t' = \lambda(t)$ for $t \in T(1+\ell\mathbb{Z}_\ell)$. It is clear that we have

$$\chi(t) \equiv 1 \bmod \ell$$

$$\chi(t)^N \equiv 1 \bmod \ell^n$$

for all $\chi \in X(T)$; from this it follows that we have $\chi(t) \equiv 1 \bmod \ell^n$ for all χ , giving $t \in T(1+\ell^n\mathbb{Z}_\ell)$.]

We find that the cokernel and kernel of λ_n are independent of n, for $n \geq 1$. Taking $n = 1$, we see that λ_1 is the map on $\mathbb{F}_\ell$ - points induced by the reduction $\lambda_{/\mathbb{F}_\ell} : T_{/\mathbb{F}_\ell} \to T'_{/\mathbb{F}_\ell}$ of λ . Thus the kernel of λ_1 is the group of $\mathbb{F}_\ell$ - rational points of the kernel of λ , so its order is in particular a *divisor* of N. On the other hand, it is well known that the kernel and cokernel of λ , have *equal* orders, because of Lang's Theorem ([5]; cf. [11] Ch.VI, n°6, Prop.5) and the triviality of the Herbrand quotient of a finite module. (Equivalently, the isogenous tori $T_{/\mathbb{F}_\ell}$ and $T'_{/\mathbb{F}_\ell}$ have the same number of rational points.) This completes the proof.

We next consider the situation where we are given tori over $\mathbb{Q}$. If $T_{/\mathbb{Q}}$ is a torus, we define $T(\mathbb{Z}/\ell^n\mathbb{Z})$ to be $T_{/\mathbb{Q}_\ell}(\mathbb{Z}/\ell^n\mathbb{Z})$ for each prime ℓ and all $n \geq 1$. Given a map $\lambda : T \to T'$ between two tori, we now write $\lambda_{\ell,n}$ for the induced maps $T(\mathbb{Z}/\ell^n\mathbb{Z}) \to T'(\mathbb{Z}/\ell^n\mathbb{Z})$.

Theorem (2.5) : *Given a torus* T *over* $\mathbb{Q}$, *there are constants* C, C' > 0 *such that we have*

$$C < \ell^{-n\nu}\,\mathrm{Card}(T(\mathbb{Z}/\ell^n\mathbb{Z})) < C'$$

for all $n \geq 1$ *and all primes* ℓ , *where* ν *is the dimension of* T.

Theorem (2.6) : *Let* $\lambda : T \to T'$ *be a surjective map between* $\mathbb{Q}$*-tori. Then the order of coker* $\lambda_{\ell,n}$ *is bounded independently of* ℓ *and* n. *If moreover* λ *is an* isogeny, the order of the ker $\lambda_{\ell,n}$ is similarly bounded.

Proofs : The second theorem is an obvious consequence of (2.3), (2.4). To prove (2.5), we will use (2.6) and a general philosophy due to Ono. First, we observe that (2.5) is visibly correct in the special case where $T = T_E$ is the torus attached to a finite extension E of $\mathbb{Q}$, cf. (2.1). Next we notice, by Brauer's theorem on induced characters, that there are finite extensions $K_1,\ldots,K_n$; $L_1,\ldots,L_m$ of $\mathbb{Q}$ and an integer r > 0 such that the two tori

$$\begin{cases} T^r \times (T_{K_1} \times\ldots\times T_{K_n}) \\ T_{L_1} \times\ldots\times T_{L_m} \end{cases}$$

are isogenous. (See [7] , Th. 1.5.1.) Since (2.5) holds for the second of the two, it holds for the first by (2.6). It thus holds for T^r (using again the case $T = T_E$) and thus for T.

Corollary (2.7) : Let $\lambda : T \to T'$ be a homomorphism of $\mathbb{Q}$-tori. There exist constants C, C' > 0 such that we have

$$C < \frac{\text{Card}(\text{Im}(\lambda_{\ell,n}))}{\ell^{n\nu}} < C'$$

for all ℓ and n, where ν is the dimension of the image of λ .

Proof : Without loss of generality, we may suppose λ surjective. Then it is clear that our result follows from (2.5) and (2.6).

3. We now wish to deduce (1.1) from the above corollary. Before beginning to do so, we make some preliminary simplifications. It is clear that to prove (1.1) for a given A/k, we may replace k by a finite extension of k and A by an abelian variety which is isogenous to it. We thus introduce the hypothesis that A has everywhere good reduction, as we have a right to do by a well known theorem of Serre-Tate ([15], Th. 7). Secondly, after replacing A by a variety isogenous to it, we may suppose that End_k A contains the "integer ring" of E. Namely, if we write E as a product $E_1 \times \ldots \times E_t$ of fields, we suppose that $\mathrm{End}_k A$ contains the product $\mathfrak{O}$ of the integer rings $\mathcal{O}_i$ of the E_i. In particular, this assumption enables us to write A as a product

$$A = A_1 \times \ldots \times A_i$$

where A_i has complex multiplication by $\mathcal{O}_i$. (It is clear that $[E_i : \mathbb{C}] = 2 \dim A_i$ for each i because the first member is known to be a divisor of the second [17, Prop.2, p.39] and because of the assumption $[E : \mathbb{Q}] = 2 \dim A$.)

It is well known (see ch. II, §.5.1 of [17]) that each A_i is isogenous over $\bar{k}$ to a power of an (absolutely) simple abelian variety B_i of CM type. In proving (1.1), we may replace each A_i by the corresponding B_i (making a finite extension of k at the same time). This enables us to assume that each of the A_i occuring above is in fact <u>absolutely</u> <u>simple</u>. This means that each of the fields E_i is a CM field and that the "CM type" attached to each A_i is simple in a sense which will be presently recalled . This assumption, and the previous ones will be in force for the remainder of this paper. To summarize, we assume :

i) that A has everywhere good reduction over k ;

ii) that A is given as a product $A_1 \times \ldots \times A_i$ of absolutely simple abelian varieties, with each A_i having complex multiplication by the integer ring of a CM field E_i.

Proving (1.1) under these assumptions will give a proof in general.

In order to discuss the individual factors with a minimum of notation, we now temporarily suppose

iii) that $t = 1$,

i.e. that A is already absolutely simple. This assumption will be in force for the remainder of this paragraph.

To discuss the "CM-type" attached to A, and the "dual" (or reflex) CM type derived from A, we embed k and E into the complex field $\mathbb{C}$. Let L be the Galois closure of E in $\mathbb{C}$, and let

$$G = \mathrm{Gal}(L/\mathbb{Q}), \quad H = \mathrm{Gal}(L/E).$$

We introduce the convention that G acts on E on the right. Thus for example, we may view the set $\mathrm{Hom}(E,\mathbb{C})$ of embeddings of E into $\mathbb{C}$ as the coset space $H\backslash G$. We write c for the complex conjugation of $\mathbb{C}$, or any of its restrictions.

As in [17], the data $(A/k,E)$ define a CM-type $S \subseteq \mathrm{Hom}(E,\mathbb{C})$. This is a subset of $H\backslash G$ such that $H\backslash G$ is the disjoint union of S and Sc . Put

$$\tilde{S} = \{g \in G \mid Hg \in S\} .$$

The absolute simplicity of A translates into the equality ([17], Prop. 26)

$$H = \{g \in G \mid g\tilde{S} = \tilde{S}\} .$$

We say that the CM type (E,S) is simple. We symetrically introduce

$$\begin{aligned} H' &= \{g \in G \mid \tilde{S}g = \tilde{S}\} \\ &= \{g \in G \mid g\tilde{R} = \tilde{R}\} , \end{aligned}$$

where $\tilde{R}$ is the set $\tilde{S}^{-1}$ of inverses of elements of $\check{S}$. Let K be the fixed field of H', and let $R \subset \mathrm{Hom}(K,\mathbb{C})$ be the image of $\tilde{R}$ in $H'\backslash G$.

Then (K,R) is again a simple CM type, that dual to (E,S). Because (E,S) is simple, it is its own double dual (i.e. the dual of (K,R)), and it is known that k contains K. (See [17] , Props. 28 and 30.)

We may view G as acting (on the right) on the set of CM types for E, and H' is then the stabilizer of the CM type (E,S). Since the number of CM types for E is 2^d where $d = [E : \mathbb{Q}]/2$ is the dimension of A, we clearly have

$$[K : \mathbb{Q}] = (G : H') \leqslant 2^d. \tag{3.1}$$

If we put $d' = [K : \mathbb{Q}]/2$, then by (3.1) and the symmetry we have

$$1 + \mathrm{Log}_2 d \leqslant d' \leqslant 2^{d-1} . \tag{3.2}$$

It is known that for each $d \geqslant 1$, we may find a CM type (E,S) with this d such that $d' = 2^{d-1}$. (For a more precise statement, see ([16], 1.10).)

Associated to the pair of CM types (E,S), (K,R) is a homomorphism

$$\phi : T_K \rightarrow T_E ,$$

which is most easily described by giving the corresponding homomorphism ϕ^* of character groups of these tori. For F a finite extension of $\mathbb{Q}$, we write X_F for the character group of the torus T_F; this is the right Gal $(\bar{\mathbb{Q}}/\mathbb{Q})$-module consisting of integral linear combinations $\Sigma\, n_\sigma\, [\sigma]$ with $\sigma \in \mathrm{Hom}(F,\mathbb{C})$. (We take $\bar{\mathbb{Q}}$ to be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.) This applies especially when F = K or E, in which case for $g \in G$ we write [g] for the embedding of F into $\mathbb{C}$ induced by g.

We define $\phi^*: X_E \rightarrow X_K$ by the formula

$$[g] \mapsto \sum_{r \in R} [rg] \cdot$$

This makes sense because replacing g by hg ($h \in H$) has the effect of permuting the various terms $[rg]$. The map ϕ^* is visibly $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-equivariant. (Cf.[17], Prop. 29.)

Following T. Kubota [4], we refer to the dimension of the image of $\phi: T_K \to T_E$ as a <u>rank</u>, the rank of the CM type (E,S). This integer may be expressed as the rank of the $\mathbb{Z}$-submodule $\phi^*(X_E)$ of X_K; using the natural bases for X_K and X_E, we then see the rank as the rank of the matrix

$$(i(\tau,\sigma))_{\substack{\sigma \in H\backslash G \\ \tau \in H'\backslash G}}$$

defined by

$$i(\tau,\sigma) = \begin{cases} 1 & \text{if } \tau\sigma^{-1} \in \tilde{R} \\ 0 & \text{if not .} \end{cases}$$

(For $\tau, \sigma \in G$, and for $h \in H$, $h' \in H'$, we have $\tau\sigma^{-1} \in \tilde{R}$ if and only if $(h'\tau)(h\sigma)^{-1} \in \tilde{R}$.) It is obvious that if we exchange the roles of (E,S) and (K,R), we replace $(i(\tau,\sigma))$ by its transpose. Hence we find

<u>Proposition (3.3)</u> : <u>The rank of a</u> CM <u>type</u> (E,S) <u>is equal to the rank of its dual</u>.

It is easy to see that the rank of (E,S) satisfies the inequality

$$\mathrm{rank}(E,S) \leqslant d+1 .$$

For example, we have $\mathrm{Im}\,\phi \subset T$, where T is the $(d+1)$-dimensional torus such that

$$T(A) = \{x \in T_E(A) = (E \otimes_{\mathbb{Q}} A)^* \mid xx^c \in A^*\}$$

for $\mathbb{Q}$-algebras A. By the symmetry (i.e. by (3.3)), we have

$$\text{(3.4)} \qquad \mathrm{rank}(E,S) \leqslant \min(d+1, d'+1).$$

These facts were all pointed out by Kubota [4], who calls a CM type non-degenerate if its rank is equal to $d+1$.

It is amusing to note that there is a lower bound for the rank :

$$\max(2+\mathrm{Log}_2 d,\ 2+\mathrm{Log}_2 d') \leqslant \mathrm{rank}(E,S). \qquad (3.5)$$

To prove (3.5), it suffices by the symmetry to prove that rank (E,S) is at least $2+\mathrm{Log}_2 d = \mathrm{Log}_2(4d)$. We note that the image of ϕ^* contains the vectors

$$\begin{cases} \sum_r [rg] & g \in H\backslash G \\ \sum_r ([r] + [rg]) & g \in H\backslash G \end{cases},$$

which we easily check to have pairwise distinct images in $X_K/2X_K$. [The only tricky point is to check that no vector in the first group is congruent mod 2 to a vector in the second. Write all vectors in the form $\sum_{g\in H'\backslash G} n_g[g]$. For vectors in the first group, we have $n_g + n_{gc} = 1$ for all g; for those in the second, we have $n_g + n_{gc} = 2$ for all g .] It follows (as Lenstra pointed out) that the image of ϕ^* generates an $\mathbf{F}_2$-subspace of $X_K/2X_K$ of dimension at least $\mathrm{Log}_2 4d$. This implies in particular the assertion about the rank.

Corollary (3.6) : Suppose that we have $d' = 2^{d-1}$. Then (E,S) is non-degenerate : we have $\mathrm{rank}(E,S) = d+1$.

Proof : We have under the hypothesis, by (3.5) and (3.4),

$$d+1 = 2+\mathrm{Log}_2 d' \leqslant \mathrm{rank}(E,S) \leqslant d+1.$$

Examples (3.7) : If d = 1,2,3, then the inequalities

$$2+\mathrm{Log}_2 d \leqslant \mathrm{rank}(E,S) \leqslant d+1$$

show that (E,S) is always non-degenerate. If d = 4, then we find

$$4 \leq \mathrm{rank}(E,S) \leq 5 ,$$

and both possibilities may occur. Indeed, if d' = 8, then the rank is 5 by (3.6) ; we may specify examples with d' = 8 as remarked after (3.2). Similarly, if d' = 3 (note that $4 = 2^{3-1}$), we have rank(E,S) = 4 by (3.6), which we apply after switching the roles of (E,S) and its dual. (Incidentally, the CM type constructed by Mumford and described in Pohlmann [9] in connection with Hodge classes on abelian varieties gives a specific example where d = 4 but d' = 3.) A case-by-case analysis once performed by the author showed that rank(E,S) is 5 in all cases where d = 4 and d' $\geq$ 4. The tedious proof of this fact has been mislaid.

Before moving to the special case where E is an abelian extension of $\mathbb{Q}$,we mention an alternate interpretation of ϕ , or rather of the composite of ϕ and the norm map $N_{k/K} : T_k \to T_K$. We let $t_{A/k}$ be the tangent space to A/k at the origin, so that $t_{A/k}$ is a k-vector space of rank d on which E acts. It is alternately an E- vector space on which k acts. For $\alpha \in k^*$ we let $\psi(\alpha) \in E^*$ be the determinant of the E-linear map "multiplication by α" on $t_{A/k}$. The map $\psi : k^* \to E^*$ is obviously induced by an algebraic map $T_k \to T_E$, which we again denote by ψ , (cf. [15], p.511).

Proposition (3.8) : The map ψ is the composition of the norm map $N_{k/K} : T_k \to T_K$ and the map $\phi : T_K \to T_E$.

This is well known, and is used implicitly in [15], § 7. For a proof, see [16], § 1.3.

Corollary (3.9) : The rank of (E,S) is equal to the dimension of the image of ψ .

Proof : The map $N_{k/K}$ is surjective .

In addition to assumptions (i),(ii), (iii) introduced above, we suppose now and for the remainder of this §, that E is an abelian extension of $\mathbb{Q}$. Then L = K = E, and G = Gal(E/$\mathbb{Q}$). We may view ϕ^* as an endomorphism of $X_E = X_K$.

We calculate the effect of ϕ^* on the basis vectors $v_\chi = \sum_{g \in G} \chi(g)[g]$ of $X_E \otimes \mathbb{C}$, where χ runs over the set of $\mathbb{C}^*$-valued characters of the abelian group G. We find

$$\phi^*(v_\chi) = \Big(\sum_{s \in S} \chi(s)\Big) v_\chi$$

for each χ. This gives

Proposition (3.10) (cf.[4], lemma 2) : The rank of (E,S) is the number of characters χ for which the sum

$$\chi(S) = \sum_{s \in S} \chi(s)$$

is non zero.

Note that when χ is an even character (i.e. $\chi(c) = +1$), we have $\chi(S) \neq 0$ if and only if χ is non trivial. The rank is thus one plus the number of odd characters χ for which $\chi(S)$ is non zero.

We close this paragraph with some examples.

(3.11) Let $p \geq 5$ be a prime, and let E be the field $\mathbb{Q}(\mu_p)$ of p^{th} roots of unity. We identify G with $(\mathbb{Z}/p\mathbb{Z})^*$ in the usual way. For $g \in G$, write $<g>$ for the integer between 1 and $p-1$ which represents g mod p. Let a be an integer satisfying $1 \leq a \leq p-2$. The set

$$S = \{g \in G \mid <g> + <ag> < p\}$$

is readily seen to be a CM type for E. It is simple if and only if a is of order $\neq 3$ in $(\mathbb{Z}/p\mathbb{Z})^*$, which we suppose to be the case. (See, e.g., [3], Th. 2.) For χ odd, one finds

$$\chi(S) = L(0, \chi)(1 + \chi^{-1}(a) - \chi^{-1}(1+a)),$$

by a computation generalizing that of [4] , lemma 3. Thus (E,S) is "degenerate" if and only if there is an odd character χ satisfying the unlikely equality

$$\chi(1+a) = \chi(1) + \chi(a) .$$

Thus S is non-degenerate, for example, if a = 1. Greenberg [2] found that S is degenerate for p = 67 and a = 10, 19, 47, 56, 60. For sufficiently large primes $p \equiv 7 \pmod{12}$, Lenstra and Stark noticed that there is always an a for which S is degenerate (loc. cit.).

(3.12) Let E be the field of 32nd roots of unity. As usual, we identify G with $(\mathbb{Z}/32\mathbb{Z})^*$. Let S be the subset $\{1, 7, 13, 15, 21, 23, 27, 29\}$ of G. Then S is a "simple" CM type, and $\chi(S)$ vanishes when χ is the character

$$x \longmapsto \begin{cases} -1 & \text{if } x \equiv 3 \pmod 4 \\ +1 & \text{if } x \equiv 1 \pmod 4 \end{cases} .$$

Thus S is degenerate . (This example was found by Lenstra.) Similarly, if we take $S' = \{1, 7, 9, 11, 13, 15, 27, 29\}$, then S' is again a simple CM type such that $\chi(S') = 0$ for <u>both</u> odd characters χ' of order 2.

(3.13) Take E this time to be the field of 19th roots of unity, so that G is $(\mathbb{Z}/19\mathbb{Z})^*$. Let $S = \{1,3,4,5,6,7,8,10,17\}$. Then S is a simple CM type such that $\chi(S) = 0$ for both (odd) characters χ of order 6. (This example was provided by Serre in response to a question of Masser.)

(3.14) Let p,q,r be distinct odd primes, and let G be the cyclic group $\mathbb{Z}/2pqr\mathbb{Z}$. Let E be a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(E/\mathbb{Q}) \simeq G$. Let S be the subset of G consisting of those elements having order 1, pqr, 2p, 2q, 2r, 2pq, 2pr, or 2qr. It is evident that (E,S) is a CM type, and it is simple because S contains the identity element of G but no non-trivial subgroup of G. A calculation shows that, for χ odd, we have $\chi(S) = 0$ if and only if χ has order 2pqr. Hence we have

$$\operatorname{rank}(E,S) = 1 + pqr - (p-1)(q-1)(r-1).$$

This example, recently constructed by Lenstra, shows that the rank may be quite small relative to $[E : \mathbb{Q}]$, even in the case where the CM field E is abelian.

4. We now return to the situation outlined at the beginning of § 3, where the abelian variety A/k satisfies conditions (i) and (ii), but we no longer assume that E is a single field. We wish to prove (1.1) for A.

For $N \geq 1$, let A_N be the $\mathrm{Gal}(\bar{k}/k)$-module of N-division points on A, and let G_N be the image of the representation

$$\rho_N : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}\, A_N$$

giving the action of $\mathrm{Gal}(\bar{k}/k)$ on A_N. Thus G_N is the Galois group over k of the division field $k(A_N)$, and the order of G_N is the degree d(N) of this field. Since A has everywhere good reduction over k, $k(A_N)/k$ is ramified only at primes of k dividing N. Thus, if N and M are relatively prime, $k(A_N) \cap k(A_M)$ is contained in the Hilbert class field of k. After replacing k by its Hilbert class field, we thus find that the function

$$N \longmapsto d(N)$$

is "multiplicative" in the usual arithmetic sense. Thus to prove (1.1) it suffices to obtain for each prime ℓ and each integer $n \geq 1$ an inequality

$$C < \frac{d(\ell^n)}{\ell^{n\nu}} < C' \tag{4.1}$$

in which C and C' are constants depending on A, k, E, and where $\nu \geq 0$ is an integer.

We recall now the decomposition $A = A_1 \times \ldots \times A_t$. For each i, let $\psi_i : T_k \longrightarrow T_{E_i}$ be the map ψ of (3.8) made with the abelian variety A of § 3 taken to be A_i. Let

$$\psi : T_k \to T_E = T_{E_1} \times \ldots \times T_{E_t}$$

be the product of the ψ_i. We will prove that (4.1) holds with ν equal to the dimension of the image of ψ. Thus if A is simple (i.e. $t = 1$), then ν is the rank of the CM type attached to A, in the sense of § 3.

For a prime ℓ, let ρ_{ℓ^∞} be the ℓ-adic representation of $\mathrm{Gal}(\bar{k}/k)$ attached to A, i.e. the projective limit of the ρ_{ℓ^n} $(n \geq 1)$. *A priori*, ρ_{ℓ^∞} takes values in the group of automorphisms of the Tate module $\varprojlim A_{\ell^n}$ of A, but it is well known that the values of ρ_{ℓ^∞} lie in the subgroup $(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^*$ of $\mathrm{Aut}(\varprojlim A_{\ell^n})$, cf. [15, § 4, Cor. 2]. Hence ρ_{ℓ^∞} is abelian and may be viewed as a map

$$I_k \longrightarrow (\mathcal{O} \otimes \mathbb{Z}_\ell)^*,$$

where I_k is the group of idèles of k. For (4.1), no harm is done in replacing I_k by the product $\prod_v U_v$ of the groups of units at the non-archimedean completions of k, since this product has finite index in the abelianized Galois group of k. (In fact, this replacement is the replacement of k by its Hilbert class field which we discussed above.) Now ρ_{ℓ^∞} kills the group U_v if v is not of residue characteristic ℓ. Hence, we will view ρ_{ℓ^∞} as a map

$$\prod_{v|\ell} U_v \longrightarrow (\mathcal{O} \otimes \mathbb{Z}_\ell)^*$$

i.e., as a map

$$T_k(\mathbb{Z}_\ell) \to T_E(\mathbb{Z}_\ell),$$

cf. (2.1).

Let $\lambda : T_k \to T_E$ be the "inverse" of ψ, i.e., the map $x \mapsto \psi(x^{-1})$. Then ρ_{ℓ^∞} is just the map on $\mathbb{Z}_\ell$-points induced by λ, in view of Theorem 11 of [15] and its corollaries. Now ρ_{ℓ^n} for $n \geq 1$ is the composition of the map

ρ_{ℓ^∞} with the reduction map $(\mathcal{O}\otimes\mathbb{Z}_\ell)^* \to (\mathcal{O}/\ell^n\mathcal{O})^*$, i.e., $T_E(\mathbb{Z}_\ell) \to T_E(\mathbb{Z}/\ell^n\mathbb{Z})$.
We have an evident commutative diagram

$$\begin{tikzcd}
T_k(\mathbb{Z}_\ell) \arrow[r] \arrow[d] & T_E(\mathbb{Z}_\ell) \arrow[d] \\
T_k(\mathbb{Z}/\ell\mathbb{Z}) \arrow[r] & T_E(\mathbb{Z}/\ell\mathbb{Z})
\end{tikzcd}$$

in which the two vertical maps are reduction maps, the top horizontal map is ρ_{ℓ^∞} and the lower horizontal map is the map denoted $\lambda_{\ell,n}$ toward the end of § 1. Hence G_{ℓ^n} is just the image of $\lambda_{\ell,n}$ (for $n > 1$), and $d(\ell^n)$ is the order of $\mathrm{Im}(\lambda_{\ell,n})$. Thus (1.1) is a special case of (2.7). Finally, again by (2.7), the integer ν of (1.1) is the dimension of the image of λ , or in other words the dimension of the image of ψ . This establishes (4.1) and the claim concerning the value of ν.

BIBLIOGRAPHY

[1] Deligne, P. , Cycles de Hodge absolus et périodes des intégrales des variétés abéliennes, rédigé par J. L. Brylinski. This volume.

[2] Greenberg, R. , On the Jacobian variety of some algebraic curves. Preprint, 1978.

[3] Koblitz, N. and Rohrlich, N. , Simple factors in the Jacobian of a Fermat curve. Canadian J. Math. 30, 1183-1205 (1978).

[4] Kubota, T. , On the field extension by complex multiplication. Trans. AMS 118, n° 6, 113-122 (1965).

[5] Lang, S. , Algebraic groups over finite fields. Am. J. Math 78 , 555-563 (1956).

[6] Masser, D. W. , On quasi-periods of abelian functions with complex multiplication. This volume.

[7] Ono, T. , Arithmetic of algebraic tori. Ann. of Math. 74, 101-139 (1961).

[8] Ono, T. , On the Tamagawa number of algebraic tori. Ann. of Math. 78 , 47-73 (1963).

[9] Pohlmann, H., Algebraic cycles on abelian varieties of complex multiplication type. Ann. of Math. 88, 161-180 (1968).

[10] Ribet, K. A. , Kummer theory on extensions of abelian varieties by tori. Duke Math. J. 46, 745-761 (1979).

[11] Serre, J. P. , Groupes Algébriques et Corps de Classes. Hermann, Paris, 1959.

[12] Serre, J. P. , Corps Locaux. Deuxième édition revue et corrigée. Hermann, Paris, 1968.

[13] Serre, J. P. , Letter to D. Masser, November, 1975.

[14] Serre, J. P. , Représentations ℓ-adiques. In Algebraic Number Theory (Int. Symp., Kyoto, 1976), Japan Society for the Promotion of Science, Tokyo, 1977.

[15] Serre, J. P. and Tate, J. , Good reduction of abelian varieties. Ann. of Math. 88, 492-517 (1968).

[16] Shimura, G. , Arithmetic quotients of bounded symmetric domains. Ann. of Math. 91, 144-222 (1970).

[17] Shimura, G. and Taniyama, Y. , Complex Multiplication of Abelian Varieties and its Applications to Number Theory. Publ. Math. Soc. Japan n°6, Tokyo, 1961.

[18] Weil, A. , On a certain type of characters of the idèle-class group of an algebraic number-field. Proc. International Symp. on Algebraic Number Theory, Tokyo-Nikko, 1-7 (1955) = Collected Papers [1955c].

Ecole Polytechnique
Centre de Mathématiques
91128 Palaiseau Cedex (France)

MÉMOIRES DE LA S. M. F.

JEAN-PIERRE SERRE

Annexe : deux lettres de Serre

Mémoires de la S. M. F. 2e série, tome 2 (1980), p. 95-102

<http://www.numdam.org/item?id=MSMF_1980_2_2__95_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 95-102

ANNEXE

DEUX LETTRES DE SERRE

Comme l'indique K. Ribet, le théorème 1.1. de son article généralise des résultats de J.-P. Serre. Ceux-ci répondaient à des questions rencontrées par D. Masser dans ses travaux sur l'indépendance linéaire de périodes et de pseudo-périodes de fonctions elliptiques (voir le chapitre 6 de "Transcendence Theory : Advances and Applications", A. Baker and D. Masser eds., Academic Press 1977). On trouvera ci-dessous l'essentiel de deux lettres de Serre à Masser sur ces questions.

La première lettre (Novembre 75) concerne le problème suivant. On désigne par $E^1,\dots,E^n$ des courbes elliptiques définies sur un corps de nombres $K \subset \bar{Q}$, admettant des multiplications complexes par des corps quadratiques imaginaires $F^1,\dots,F^n \subset \bar{Q}$. On suppose que les corps F^i sont deux à deux distincts, de sorte que les courbes elliptiques E^i sont deux à deux non isogènes sur $\bar{Q}$. Soit K^{cycl} l'extension de K engendrée par toutes les racines de l'unité de $\bar{Q}$. Pour $i = 1,\dots,n$, on note E^i_∞ le groupe des points de torsion de $E^i(\bar{Q})$ et $K(E^i_\infty)$ l'extension de K engendrée par les coordonnées des points de E^i_∞ ; les corps $K(E^i_\infty)$ contiennent K^{cycl}. D'après un résultat connu (cf. e.g. Serre, Invent. Math. 15, 259-331, Théorème 7) les extensions $K(E^i_\infty)/K^{cycl}$ sont presque disjointes deux à deux : pour tout couple (i,j) d'indices distincts, $K(E^i_\infty) \cap K(E^j_\infty)$ est une extension finie de K^{cycl}. Dans quelle mesure est-il encore vrai que les $K(E^i_\infty)/K^{cycl}$ sont presque disjointes "dans leur ensemble", i.e. que $K(E^i_\infty)$ est presque disjointe sur K^{cycl} du composé des $K(E^j_\infty)$, pour $j \neq i$?

[...] Distinguons deux cas :

a) Cas "agréable" . Les F^i sont non seulement distincts, mais même linéairement disjoints (i.e. aucun d'eux n'est contenu dans le composé des autres - cela exclut, par exemple, le cas de courbes elliptiques à mult. complexe par $Q(\sqrt{-a})$, $Q(\sqrt{-b})$, $Q(\sqrt{-c})$ et $Q(\sqrt{-abc})$.

Alors les extensions $K(E^i_\infty)/K^{cycl}$ $(i = 1,\dots,n)$ sont presque disjointes.

b) <u>Cas général</u> . On ne fait aucune hypothèse sur les F^i. La situation est un peu moins bonne. Pour la préciser, supposons K assez grand pour contenir les F^i (de sorte qu'on a des extensions abéliennes) ; posons $G^i_N = \mathrm{Gal}(K^{cycl}(E^i_N)/K^{cycl})$, où E^i_N est le groupe des points de division par N dans E^i, et soit G_N le groupe de Galois sur K^{cycl} de l'extension composée des $K^{cycl}(E^i_N)$ pour $i = 1,\dots,N$, de sorte que G_N s'identifie à un sous-groupe du produit $G^1_N \times\dots\times G^n_N = H_N$. La presque disjonction équivaudrait à l'affirmation que l'indice de G_N dans H_N est borné ; en fait, ce n'est pas exact, on peut simplement affirmer ceci : <u>il existe des constantes</u> A <u>et</u> B <u>telles que</u> $(H_N:G_N)$ <u>soit un diviseur de</u> $A.B^{r(N)}$, <u>où</u> r(N) <u>est le nombre de facteurs premiers</u> (distincts) <u>de</u> N; de plus, on peut prendre pour B une puissance de 2 (i.e. il y a presque disjonction, à des 2-groupes près).

Notez que $r(N) = 1$ si $N = \ell^m$, ℓ premier, $m \geqslant 1$ arbitraire : l'indice de G_{ℓ^m} dans H_{ℓ^m} est donc <u>borné</u> par une constante indépendante de ℓ et de m ; n'est-ce pas suffisant pour les applications ? Cela me parait très probable.

<u>Esquisse de la démonstration</u>

Quitte à agrandir K, on peut supposer qu'il contient les F^i et que les E^i ont bonne réduction. Si ℓ est un nombre premier, je note $U_\ell(K)$ le produit des groupes des unités $U(K_v)$, pour $v|\ell$, où K_v est le complété de K en v (c'est le sous-groupe compact maximal du groupe des éléments inversibles de l'algèbre $Q_\ell \otimes K = K_\ell$); j'écris U_ℓ si $K = Q$.

Toutes les extensions considérées sont abéliennes ; on peut donc considérer que ce sont les groupes d'idèles des corps considérés qui opèrent. En particulier, si $u \in U_\ell(K)$, on sait que l'action de u sur E^i_∞ est triviale sur les ℓ'-composantes de E^i_∞ pour $\ell' \neq \ell$, et qu'elle est donnée par la multiplication par $N_i(u^{-1})$ sur la ℓ-composante, où N_i est la norme de K à F^i (on a $N_i(u^{-1}) \in U_\ell(F^i)$); ce résultat est classique (voir par exemple mon article à Inventiones, fin du § 4).

Il résulte de ceci que le groupe $G^i = \varprojlim . G^i_N$ s'identifie à un sous-groupe d'indice fini du groupe $U'(F^i) = \prod_\ell U'_\ell(F^i)$, où je note $U'_\ell(F^i)$ le sous-groupe de

$U_\ell(F^i)$ formé des éléments dont la norme dans U_ℓ est égale à 1.

On est donc ramené à considérer le problème suivant :

Soit ℓ un nombre premier. Notons $U'_\ell(F)$ le sous-groupe de $U_\ell(K)$ formé des éléments de norme 1 dans U_ℓ. Considérons l'application

$$f_\ell : U'_\ell(K) \to U'_\ell(F^1) \times\ldots\times U'_\ell(F^n)$$

donnée par $u \mapsto (N_1(u),\ldots,N_n(u))$.

Est-il vrai que $\mathrm{Im}(f_\ell)$ est <u>ouverte</u> pour tout ℓ, et que, pour presque tout ℓ, l'indice de $\mathrm{Im}(f_\ell)$ est <u>borné</u> par une constante B que l'on peut prendre égale à 1 dans le cas a) ?

C'est là un problème de nature élémentaire, mais un peu ennuyeux à traiter en détail en dehors des cas $n = 1,2$ qui sont faciles. Si l'on veut se fatiguer le moins possible, on peut utiliser un peu de géométrie algébrique, de la manière suivante :

Soit T un tore sur Q, de groupe des caractères X; j'entends par là un Q-groupe algébrique, qui est $\bar{Q}$-isomorphe à un produit de groupes multiplicatifs G_m ; on a $X = \mathrm{Hom}_Q(T,G_m)$, c'est un Z-module libre sur lequel agit $\mathrm{Gal}(\bar{Q}/Q)$, et sa connaissance équivaut à celle de T. Si ℓ est un nombre premier, je note $T(Q_\ell)$ le groupe des Q_ℓ -points de T, et $T^c(Q_\ell)$ le sous-groupe compact maximal de $T(Q_\ell)$.

(Exemple : si K est un corps de nombres comme ci-dessus, et si je prends pour X le groupe libre de base l'ensemble des plongements de K dans $\bar{Q}$, je trouve pour T un tore T_K qui a la vertu que $T_K(Q_\ell) = (K \otimes Q_\ell)^*$, et $T_K^c(Q_\ell) = U_\ell(K)$.)

Soit maintenant $f : T_1 \to T_2$ un homomorphisme de tores, correspondant à un homomorphisme $\hat{f} : X_2 \to X_1$ des groupes de caractères correspondants. On suppose f surjectif (au sens géom.alg.), i.e. $\hat{f}$ injectif ; on identifie ainsi X_2 à un sous-groupe de X_1. Notons N le noyau de f, N^o la composante neutre de N, et B l'ordre du groupe fini N/N^o; l'entier B a une interprétation simple en termes de X_1 et X_2 :

si l'on désigne par $\tilde{X}_2$ le sous-groupe de X_1 formé des éléments $x \in X_1$ tels qu'il existe $m \geq 1$ avec $mx \in X_2$, B n'est autre que l'ordre de $\tilde{X}_2/X_2$, i.e. l'ordre du sous-groupe de torsion de X_1/X_2.

Ceci étant, si ℓ est premier, f définit un homomorphisme

$$f_\ell : T_1^c(Q_\ell) \to T_2^c(Q_\ell) \quad ,$$

et l'on a :

Lemme- i) Pour tout ℓ, l'homomorphisme f_ℓ est ouvert. En particulier, son image est d'indice fini.

ii) Pour presque tout ℓ , l'indice de $\mathrm{Im}(f_\ell)$ est un diviseur de l'entier B défini plus haut.

L'assertion i) est immédiate : l'application tangente à f à l'élement neutre est en effet surjective, et l'on applique la théorie des groupes de Lie - ou tout autre argument ! L'assertion ii) n'est guère plus difficile ; pour presque tout ℓ , on a bonne réduction et $T^c(Q_\ell)$ peut s'interpréter comme $T(Z_\ell)$, groupe des points entiers en ℓ. L'application f_ℓ est surjective pour les points congrus à 1 mod. ℓ (argument de Lie, de nouveau) ; le conoyau se voit sur la réduction mod. ℓ et l'on est ramené à un énoncé sur les corps finis, qui est facile. (On peut sûrement trouver les détails de ceci dans les articles d'Ono aux Annals en 1961, 63,65.) Un cas typique, qui fait bien comprendre ce qui se passe, est celui de l'isogénie $f : x \mapsto x^2$ entre G_m et G_m : l'indice $(U_\ell : U_\ell^2)$ est égal à 2 (c'est-à-dire à l'ordre du noyau de f) pour tout $\ell \neq 2$.

Vous voyez comment ce lemme s'applique ici : on prend pour T_1 le tore T'_K noyau de l'homomorphisme "norme" $T_K \to T_Q = G_m$, où T_K est le tore défini plus haut "groupe multiplicatif de K" ; on prend pour T_2 le produit des tores à une dimension T'_{F^i} ; on prend pour

$$f : T'_K \to \prod_{i=1}^{n} T'_{F^i}$$

l'application définie par les normes N_i.

La surjectivité de f est facile; d'où l'existence de B. Il faut un peu plus travailler pour prouver que B est une puissance de 2, et que B est même égal à 1 dans le cas "agréable" du début; cela se fait de la façon la plus commode en explicitant les groupes de caractères X_1 et X_2 . [...]

[J'aurais sans doute dû dire pourquoi j'ai le droit de me borner à regarder l'action de $\prod_\ell U_\ell(K)$ sur les E^i_∞ : c'est que l'image de ce groupe dans $\mathrm{Gal}(K^{ab}/K)$ est un sous-groupe <u>d'indice fini</u> h (nombre de classes), et que toute la question est "à un groupe fini près".]

La deuxième lettre (Juin 76) concerne le corps $\mathcal{K}_\ell$ engendré par les coordonnées des points d'ordre ℓ premier d'un produit de courbes elliptiques à multiplications complexes. On suppose que les hypothèses du "cas agréable" de la première lettre sont vérifiées. D'après le résultat de cette lettre, le degré de $\mathcal{K}_\ell$ sur K est "aussi grand que possible" pour presque tous les nombres premiers ℓ . On trouvera ci-dessous une démonstration plus explicite de cette assertion. Les corps quadratiques F^i sont maintenant notés k_i .

[...] I start with quadratic imaginary fields $k_1,\dots,k_n$ contained in a number field K. I put $D = |\mathrm{disc}(K)|$. I assume the k_i's are independent, i.e. that they generate a field k whose degree is 2^n.

Take $\ell \nmid D$, so that ℓ is unramified in K and the k_i's. Denote by $k_i(\ell)$ the quotient of the ring of integers of k_i by the ideal generated by ℓ . We have :

$$k_i(\ell) = \begin{cases} F_\ell \times F_\ell & \text{if } \ell \text{ splits in } k_i \\ F_{\ell^2} & \text{if } \ell \text{ is inert in } k_i. \end{cases}$$

Define similarly $k(\ell)$ and $K(\ell)$; these are finite rings, products of fields corresponding to the prime ideals above ℓ. We have norm homomorphisms

$$N_{K/k_i} : K(\ell)^* \to k_i(\ell)^* \text{ and } \quad N_{k_i/Q} : k_i(\ell)^* \to F_\ell^*.$$

Putting together the N_{K/k_i} $(i = 1,\dots,n)$, we get a homomorphism

$$N_K : K(\ell)^* \to k_1(\ell)^* \times \dots \times k_n(\ell)^*.$$

Lemma : *The image of* N_K *is the set of* $(x_1,\dots,x_n)$, $x_i \in k_i(\ell)^*$, *such that* $N_{k_1/Q}(x_1) = \dots = N_{k_n/Q}(x_n)$ *in* F_ℓ .

Call V the set of (x_i) with the property $N_{k_1/Q}(x_1) = \dots = N_{k_n/Q}(x_n)$. It is clear that $\mathrm{Im}(N_K) \subset V$. To prove the converse, we may assume that K is equal to $k = k_1 \dots k_n$; indeed it is well known that $N_{K/k} : K(\ell)^* \to k(\ell)^*$ is surjective. Use now induction on n, starting with n = 0, which is trivial.

If $(x_i) \in V$, induction shows that there is $y \in k(\ell)^*$ with $N_{k_2/Q}(y) = x_2$, $\dots, N_{k_n/Q}(y) = x_n$. This allows us to reduce the problem to the case where $x_2 = \dots = x_n = 1$, in which case we have $N_{k_1/Q}(x_1) = 1$. But, if we call $s_1,\dots, s_n$ the obvious generators of Gal(k/Q) (so that s_i is trivial on k_j if and only if $j \neq i$), it is elementary that $N_{k_1/Q}(x_1) = 1$ implies the existence of $z_1 \in k_1(\ell)^*$ with $z_1^{1-s_1} = x_1$. Now, use the surjectivity of the norm map $N_{k/k_1} : k(\ell)^* \to k_1(\ell)^*$, and get $t \in k(\ell)^*$ with $N_{k/k_1}(t) = z_1$. Put $y = t^{1-s_1}$. I claim that y does the trick. Indeed :

$$N_{k/k_1}(y) = N_{k/k_1}(t)^{1-s_1} = z_1^{1-s_1} = x_1$$

$$N_{k/k_i}(y) = y^{(1+s_1)(1+s_2)\dots(1+s_{i-1})(1+s_{i+1})\dots(1+s_n)} = 1 \qquad (i > 2).$$

This proves the lemma.

(We could replace Q by any number field, and the k_i by any Galois extensions of that field -provided those extensions were linearly disjoint. But the above statement will be enough.)

Now I come to elliptic curves E_i $(1 \leqslant i \leqslant n)$, with complex multiplications by some orders O_i of k_i, and defined over the number field K. I will say that ℓ is large if :

a) $\ell \nmid D$ (as above),

b) ℓ does not divide any of the conductors of the orders O_i,

c) each E_i has good reduction at all the primes of K dividing ℓ . (Thus, we exclude a finite constructible set of bad primes ℓ.)

Call $E_i(\ell)$ the group of ℓ-division points of E_i ; by b), we have an action of $k_i(\ell)$ on $E_i(\ell)$, which makes it a free $k_i(\ell)$-module of rank 1. Hence the action of $Gal(\bar{K}/K)$ on $E_i(\ell)$ factors through a homomorphism

$$\rho_i : Gal(\bar{K}/K) \to k_i(\ell)^* .$$

The collection (ρ_i) defines a homomorphism :

$$\rho : Gal(\bar{K}/K) \to k_1(\ell)^* \times \ldots \times k_n(\ell)^* .$$

<u>Main Lemma</u> : <u>If</u> ℓ <u>is large</u>, <u>the image of</u> ρ <u>is equal to the set</u> V <u>of</u> (x_i) <u>with</u> $N_{k_1/Q}(x_1) = \ldots = N_{k_n/Q}(x_n)$, <u>as in the previous lemma</u>.

First, it is well known that $N_{k_i/Q} \circ \rho_i : Gal(\bar{K}/K) \to F_\ell^*$ gives the action of that Galois group on the ℓ-th roots of unity. Hence it is independent of the choice of i, and we have $Im(\rho) \subset V$. To prove the converse, one looks at the action of the <u>inertia group</u> at ℓ on the $E_i(\ell)$'s. More precisely, since the action is abelian, by class field theory we may interpret each ρ_i (and hence ρ) as a homomorphism from the idèle group of K ; inside this group, we have $K_\ell^* = \prod_{\underline{p}|\ell} K_{\underline{p}}^*$, and its unit group $U_\ell = \prod_{\underline{p}|\ell} U_{\underline{p}}$. We have a natural homomorphism $U_\ell \to K(\ell)^*$, given by reduction mod. ℓ . Now the theory of elliptic curves with complex multiplications tells us that,if $u \in U_\ell$, and if $\bar{u}$ is its image in $K(\ell)$, we have

$$\rho_i(u^{-1}) = N_{K/k_i}(\bar{u}) \quad \text{in } k_i(\ell)^* \text{ for all } i .$$

Hence, the main lemma follows from the elementary lemma above. [...]

[Two more remarks :

1 - One can prove that condition b) above is implied by conditions a) and c).

2 - If one does not assume that the fields k_i are independent, but merely that they are pairwise distinct, one can easily prove the following result (which is probably strong enough for applications to transcendency problems) : there exists constants A,B (depending only on the number n of elliptic curves), such that, for every ℓ large enough (depending on n and the curves), the order of the Galois group $\mathrm{Im}(\rho)$ is such that :

$$A\,\ell^{n+1} < |\mathrm{Im}(\rho)| < B\,\ell^{n+1} .$$

Moreover, A, B and "large enough" are effectively computable.]

J.-P. Serre
Collège de France
11, place Marcelin Berthelot
75005 Paris

MÉMOIRES DE LA S. M. F.

GORO SHIMURA

The periods of abelian varieties with complex multiplication and the spectral values of certain zeta functions

Mémoires de la S. M. F. 2^{e} série, tome 2 (1980), p. 103-106

<http://www.numdam.org/item?id=MSMF_1980_2_2__103_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 103-106

THE PERIODS OF ABELIAN VARIETIES WITH COMPLEX MULTIPLICATION AND THE SPECIAL VALUES OF CERTAIN ZETA FUNCTIONS

by

Goro SHIMURA

Let K be a CM-field of degree 2n and I_K the free $\mathbb{Z}$-module generated by all embeddings of K into $\mathbb{C}$. Given a CM-type $\varphi = \sum_{i=1}^{n} \tau_i$ of K, take a $\overline{\mathbb{Q}}$-rational abelian variety of type (K,φ) and a $\overline{\mathbb{Q}}$-rational holomorphic 1-form ω_i on A such that $\omega_i \cdot a = a^{\tau_i} \omega_i$ for all $a \in K$. As shown in [2, p.383], there is a non-zero complex number $p_K(\tau_i,\varphi)$ depending only on K,φ, and τ_i such that

$$[\pi . p_K(\tau_i,\varphi)]^{-1} \int_c \omega_i \in \overline{\mathbb{Q}}$$

for every $c \in H_1(A,\mathbb{Z})$. The quantity $p_K(\tau_i,\varphi)$ can actually be chosen to be a positive real number; it is also given as the value of a certain $\overline{\mathbb{Q}}$-rational (meromorphic) Hilbert modular form at a CM-point (see [2]). Now denote by ρ the complex conjugation, and put $r_K(\tau_i \rho,\varphi) = p_K(\tau_i,\varphi)^{-1}$. Then we have

Theorem 1 : *If $\varphi_1,\dots,\varphi_m$ are CM-types of K and τ is an embedding of K into $\mathbb{C}$, the product $\prod_{i=1}^{m} p_K(\tau,\varphi_i)^{s_i}$ with $s_i \in \mathbb{Z}$, up to algebraic factors, depends only on τ and $\sum_{i=1}^{m} s_i\varphi_i$. Moreover, if L is a CM-field containing K and ψ is a CM-type of L whose restriction to K is $\sum_{i=1}^{m} s_i\varphi_i$, then the above product equals, up to algebraic factors, to $\prod_{\sigma} p_L(\sigma,\psi)$, where σ runs over all embeddings of L into $\mathbb{C}$, which coincide with τ on K.*

The proof is given in [3] . To express this theorem in a different way, we consider two linear maps

$$\mathrm{Res}_{L/K} : I_L \longrightarrow I_K \quad , \quad \mathrm{Inf}_{L/K} : I_K \longrightarrow I_L .$$

Here $\mathrm{Res}_{L/K}(\sigma)$ is the sum of all restrictions of σ to K; $\mathrm{Inf}_{L/K}(\tau)$ is the sum of all extensions of τ to L.

Theorem 2 : *The above p_K can be extended to a bilinear map of $I_K \times I_K$ into $\mathbb{C}^\times/\overline{\mathbb{Q}}^\times$ with the following properties* :

1) $p_K(\alpha\rho,\beta) = p_K(\alpha,\beta\rho) = p_K(\alpha,\beta)^{-1}$ *for* $\alpha,\beta \in I_K$;

2) $p_K(\alpha,\mathrm{Res}_{L/K}\beta) = p_L(\mathrm{Inf}_{L/K}\alpha\ ,\beta)$, $p_K(\mathrm{Res}_{L/K}\beta\ ,\alpha) = p_L(\beta,\mathrm{Inf}_{L/K}\alpha)$ *for* $\alpha \in I_K$, $\beta \in I_L$, *and* $K \subset L$;

3) $p_M(\gamma\alpha,\gamma\beta) = p_K(\alpha,\beta)$ *if* γ *is an isomorphism of* M *onto* K.

Theorem 3 : *If* (L,ψ) *is the reflex of* (K,φ), *we have* $p_K(\sigma,\varphi) = p_L(\psi\sigma,\mathrm{id}_L)$ *for every embedding* σ *of* K *into* $\mathbb{C}$.

These theorems imply various algebraic relations among the periods. For example, we have :

Theorem 4 : For $\alpha \in I_K$, let $t(\alpha)$ denote the rank of the module $\sum_{\gamma \in G} \mathbb{Z}\alpha\gamma$, where G is the Galois group over $\mathbb{Q}$ of the Galois closure of K. If $\sum_{i=1}^{n} \tau_i$ is a CM-type of K, then for every $\beta \in I_K$, the module

$$\{(e_1,\dots,e_n) \in \mathbb{Z}^n \mid \prod_{i=1}^{n} p_K(\tau_i,\beta)^{e_i} = 1\}$$

has rank at least $n-t(\beta-\beta\rho)$.

If β is a CM-type, we have $t(\beta-\beta\rho) = t(\beta) - 1$. Theorems 2, 3 and 4 will be proved in [4].

The quantities p_K occur as the values of an L-function of a CM-field with an algebraic valued Hecke character of infinite order (see [1, Theorem 2]). As a new example of a zeta function whose values are given by p_K, we consider

$$D(s) = \sum_{0 \neq x \equiv a(\Lambda)} \mu(\mathrm{Tr}_{K/\mathbb{Q}}(yxx^{\rho}))x^{\Phi}(x^{\tau})^{-k}|x^{\tau}|^{-2s} \qquad (s \in \mathbb{C}).$$

Here Λ is a lattice in K and $a \in K$; $0 < k \in \mathbb{Z}$; τ is an embedding of K into $\mathbb{C}$; μ denotes the Fourier coefficients of an elliptic modular form $g(z) = \sum\mu(b)e^{2\pi ibz}$; y is a real element of K such that y^{τ} is its only positive conjugate; Φ is an element of I_K with non-negative coefficients.

Theorem 5 : The series D is convergent for sufficiently large Re(s) and can be continued to a meromorphic function on the whole plane.

Theorem 6 : Suppose that g is a cusp form of weight ℓ, $\mu(b)$ are all algebraic, and τ and $\tau\rho$ occur in Φ with the same multiplicity, say q. Let m be an integer such that

$$(2n - 1 - k + \ell + \deg(\Phi))/2 < m \leq q .$$

Then D(m) is $\pi^k p_K(k\tau - \Phi, 2\tau)$ times an algebraic number.

A more general result holds for a series of a similar type with a Hilbert modular form (which is not necessarily a cusp form) in place of g. The details will be given in [4].

References

[1] G. Shimura, On some arithmetic properties of modular forms of one and several variables, Ann. of Math. 102 (1975), 491-515.

[2] G. Shimura, On the derivatives of theta functions and modular forms, Duke Math. J. 44 (1977), 365-387.

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

[4] G. Shimura, The arithmetic of certain zeta functions and automorphic forms on orthogonal groups, to appear in Ann. of Math., 110 (1980) .

Princeton University
Department of Mathematics
Princeton, N. J. 08540
(U. S. A.)

MÉMOIRES DE LA S. M. F.

D. BERTRAND

M. WALDSCHMIDT

Quelques travaux récents en théorie des nombres transcendants

Mémoires de la S. M. F. 2e série, tome 2 (1980), p. 107-119

<http://www.numdam.org/item?id=MSMF_1980_2_2__107_0>

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
2e série, Mémoire n° 2, 1980, p. 107-119

QUELQUES TRAVAUX RÉCENTS EN THÉORIE DES NOMBRES TRANSCENDANTS

par

D. BERTRAND

et

M. WALDSCHMIDT

Ces dernières années, l'étude des problèmes arithmétiques liés aux fonctions abéliennes a fait quelques progrès grâce à la théorie des nombres transcendants. Motivée, entre autres, par des questions de géométrie diophantienne ou d'indépendance algébrique, cette étude s'est particulièrement développée dans le cadre des variétés abéliennes de type C.M. Certains des résultats obtenus s'étendent néanmoins aux variétés abéliennes à multiplications réelles.

De façon plus générale, après les travaux de S. Lang, on peut interpréter de façon naturelle de nombreux problèmes de transcendance en termes de groupes algébriques commutatifs connexes. Ce point de vue conduit à de nouveaux résultats de transcendance sur les intégrales abéliennes. Ainsi M. Laurent vient de démontrer la transcendance des périodes non nulles d'intégrales elliptiques de troisième espèce.

En liaison avec l'étude des courbes de Fermat, M. Laurent a obtenu d'autre part une mesure de transcendance pour les valeurs de la fonction bêta en des points rationnels. Pour les nombres transcendants liés aux courbes elliptiques, E. Reyssat a donné une liste très complète de mesures de transcendance.

Ces inégalités diophantiennes sont utiles pour les problèmes d'indépendance algébrique, domaine qui a connu, grâce à G.V. Choodnovsky, de remarquables progrès depuis quelques années. Un énnoncé p-adique vient d'être démontré par P. Philippon, qui généralise à ce propos un "lemme de zéros" de D.W. Masser. Enfin E. Reyssat a obtenu des résultats d'indépendance algébrique liés aux intégrales elliptiques de troisième espèce.

L'étude des problèmes diophantiens en dimension supérieure requiert de bons lemmes de Schwarz en plusieurs variables. Une contribution importante à ce problème vient d'être fournie par J.C. Moreau.

TRAVAUX RÈCENTS

§1. Variétés abéliennes

a) Problèmes diophantiens

On sait, depuis le mémoire de Siegel de 1929, que l'ensemble des points entiers sur une courbe de genre ≥ 1 est fini. L'une des motivations fondamentales de nombreux travaux sur les nombres transcendants est de rendre cet énoncé effectif. Nous mentionnerons ici seulement une méthode, suggérée par Lang en 1964, et nous nous limiterons aux courbes de genre 1. Cette méthode repose sur une connaissance d'une base du groupe de Mordell-Weil d'une part, et sur une inégalité diophantienne (minoration d'une forme linéaire d'intégrales elliptiques) d'autre part. Une telle inégalité est maintenant disponible dans le cas de multiplication complexe, grâce aux travaux de Masser notamment. Pour pallier la non-effectivité du théorème de Mordell-Weil, on est amené à admettre la conjecture de Birch et Swinnerton-Dyer. Les détails viennent d'être explicités par H. Groscot [3], qui démontre par exemple l'énoncé suivant :

pour tout $\varepsilon > 0$ il existe une constante $C_\varepsilon > 0$ effectivement calculable ne dépendant que de ε ayant la propriété suivante. Soit $k \in \mathbb{Z}$, $k \neq 0$ tel que la courbe elliptique $y^2 = x^3 + k$ satisfasse la conjecture de Birch et Swinnerton-Dyer. On suppose de plus que cette courbe a pour rang 1, et on note N son conducteur. Si (x,y) est un point entier sur la courbe, alors

$$\max(|x|,|y|) \leq \exp\{C_\varepsilon N^{\frac{3}{4}+\varepsilon} |k|^{\frac{1}{2}+\varepsilon}\} .$$

Le résultat inconditionnel de Stark est

$$\max(|x|,|y|) \leq \exp\{C_\varepsilon |k|^{1+\varepsilon}\} .$$

D'autres résultats dans cette direction ont été annoncés par G.V. Choodnovsky (qui admet, en plus, l'hypothèse de Riemann généralisée).

b) Matrice des périodes

Soit Ω une matrice des périodes associée à une variété abélienne A définie sur $\overline{Q}$. Tout cycle algébrique sur une puissance de A fournit une relation algébrique satisfaite par les coefficients $\{\omega_{ij}\}$ de Ω . Une conjecture de Grothendieck affirme que l'idéal engendré par ces relations est un idéal de définition de $\{\omega_{ij}\}$. Dans cette direction, Choodnovsky [2] a démontré que le degré de transcendance δ du corps engendré sur $\mathbb{Q}$ par les coefficients de Ω et d'une matrice de pseudopériodes associée à Ω est ≥ 2. Cet énoncé est particulièrement intéressant dans le cas des variétés de type CM , où de bonnes majorations de δ sont connues (voir les exposés de Deligne et de Shimura, et, pour un cas particulier classique, le §4 ci-dessous et la conjecture de Röhrlich).

c) Multiplications réelles

La méthode élaborée par Lang (voir [8]) pour l'étude des variétés abéliennes de type CM peut être généralisée aux cas des variétés abéliennes A à multiplications réelles. Une telle variété est définie par la condition suivante : il existe un plongement d'un corps de nombres totalement réel F, de degré égal à la dimension de A , dans l'algèbre d'endomorphismes $\mathrm{End}_o A$ de A. Supposons A définie sur $\overline{\mathbb{Q}}$, et notons D une base de $\mathrm{Lie}\, A(\overline{\mathbb{Q}})$ formée de vecteurs propres pour l'action de F, et exp l'application exponentielle sur $A(\mathbb{C})$. On peut alors énoncer (voir [1]) :

Théorème 1.1 : on suppose que A est une variété abélienne à multiplications réelles, définie sur $\overline{\mathbb{Q}}$, et simple. Soit u un élément de $\mathrm{Lie}\, A(\mathbb{C})$ dont l'image par exp appartienne à $A(\overline{\mathbb{Q}})$. Si u est non nul, chacune de ses composantes dans la base D est transcendante.

Cet énoncé permet d'étudier les intégrales abéliennes de première espèce prises sur une courbe modulaire, et, en particulier, les valeurs de certaines fonctions L automorphes. Bien entendu, il permet également de retrouver la transcendance des nombres B(a,b), quand a et b sont des nombres rationnels non entiers (voir §4).

Signalons enfin que la condition de simplicité peut être supprimée dans les hypothèses du théorème 1.1.

§2. Groupes algébriques

Les principaux résultats classiques de transcendance concernant les fonctions exponentielles, elliptiques ou abéliennes peuvent être énoncés en termes de groupes algébriques commutatifs connexes. Ainsi les théorèmes de Hermite Lindemann et Gel'fond Schneider sur la fonction exponentielle, et de Schneider sur les fonctions elliptiques ainsi que le théorème 1.1. ci-dessus, sont des cas particuliers de l'énoncé suivant

Théorème 2.1 : Soit G un groupe algébrique commutatif connexe défini sur le corps $\overline{\mathbb{Q}}$ des nombres algébriques. Soit $\varphi : \mathbb{C}^n \to G_{\mathbb{C}}$ un homomorphisme analytique dont l'application linéaire tangente à l'origine est injective et définie sur $\overline{\mathbb{Q}}$. S'il existe n nombres complexes $t_1,\ldots,t_n$, $\mathbb{C}$-linéairement indépendants, tels que $\varphi(t_j) \in G_{\overline{\mathbb{Q}}}$, $(1\leq j\leq n)$, alors $\varphi(\mathbb{C}^n)$ est un sous-groupe algébrique fermé de dimension n de $G_{\mathbb{C}}$.

Cet énoncé se trouve dans le livre de Lang sur les nombres transcendants avec l'hypothèse supplémentaire que l'application exponentielle de G peut être représentée par des fonctions méromorphes d'ordre fini, mais J.P. Serre a montré ([8], Appendice II) qu'une telle représentation existe toujours, avec des fonctions d'ordre ≤ 2.

Dans le cas où G est extension d'une courbe elliptique par le groupe multiplicatif, cette représentation fait intervenir, outre la fonction elliptique $\wp$ de Weierstrass associée à la courbe, une fonction méromorphe multiplicativement quasi-périodique :

$$f(u,z) = \frac{\sigma(z-u)}{\sigma(z)\sigma(u)}\, e^{z\zeta(u)}$$

qui satisfait

$$f(u,z+\omega) = f(u,z)\ e^{\omega\zeta(u)-\eta u}$$

pour toute période ω .

Du théorème 2.1 avec $n=1$ on déduit alors facilement [8] :

Corollaire 2.2. : Soient $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, ω une période non nulle de $\wp$, u un nombre complexe dont aucun multiple rationnel n'est période de $\wp$, et β un nombre algébrique. Alors le nombre

$$\exp\{\omega\zeta(u) - \eta u + \beta\omega\}$$

est transcendant.

En particulier on obtient la transcendance du nombre $\zeta(u) - \frac{\eta}{\omega} u$, résultat dû à Choodnovsky [2] (cf. § 5 ci-dessous).

§3. Intégrales elliptiques de troisième espèce

Le corollaire 2.2 peut être formulé sous la forme suivante. Soit w une période non nulle d'une forme différentielle elliptique de troisième espèce définie sur $\overline{\mathbb{Q}}$ et dont les résidus sont rationnels. Alors e^w est soit une racine de l'unité, soit un nombre transcendant. La transcendance du nombre w lui-même vient d'être démontrée par M. Laurent [4] (cf. le troisième problème du livre de Schneider sur les nombres transcendants). Avec les hypothèses du corollaire 2.2, l'énoncé précis de Laurent est le suivant.

Théorème 3.1 : Les 4 nombres $1, \omega, \eta, \eta u - \omega\zeta(u)$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$. De plus, dans le cas de multiplication complexe, les 5 nombres $1, \omega, \eta, \eta u - \omega\zeta(u)$ et $2i\pi$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.

La démonstration de Laurent repose pour une bonne part sur les idées de D.W. Masser, qui avait résolu le problème de l'indépendance linéaire de périodes d'intégrales elliptiques de première ou de deuxième espèce en démontrant que les 6 nombres $1, \omega_1, \omega_2, \eta_1, \eta_2, 2i\pi$ engendrent un espace vectoriel sur $\overline{\mathbb{Q}}$ de dimension 6 quand il n'y a pas de multiplication complexe, et 4 dans le cas de multiplication complexe.

Une autre difficulté qui intervient dans la démonstration du théorème 3.1 est la nécessité d'expliciter les relations de multiplication exprimant $f(u,nz)/f(u,z)^n$ comme fonction rationnelle de $\wp(z)$, $\wp'(z)$, $\wp(u)$, $\wp'(u)$. Ces estimations ont été faites par E. Reyssat qui a obtenu une mesure de transcendance pour le nombre du corollaire 2.2.

Enfin Laurent a besoin d'un "lemme de zéros" pour lequel il a adapté des arguments de Masser, ce qui lui permet de démontrer le résultat suivant.

Proposition 3.2 : *Soit* $P \in \mathbb{C}[x_o,x_1,x_2,x_3]$ *un polynôme non nul de degré* $\leq L$. *Sous les hypothèses du corollaire* 2.2, *on définit*

$$g(z) = az + b\zeta(z)$$

où a,b *sont deux nombres complexes non tous deux nuls*, *et*

$$f(z) = \frac{\sigma(z-u)}{\sigma(z)\ \sigma(u)} \exp\left(\frac{\eta u}{\omega} z\right)$$

Alors pour tout $R > 0$ *le nombre de zéros dans le disque* $|z| \leq R$ *de la fonction*

$$P(g(\omega z),\ \wp(\omega z),\ f(\omega z),\ e^{2i\pi z})$$

est majoré par $c(LR^2 + R^8)$, *où* c *ne dépend que de* $\wp$, u, ω, a *et* b .

§4. Mesures de transcendance

Soient $\mathcal{C}$ une courbe algébrique de genre g dans $\mathbb{P}_2(\mathbb{C})$, définie sur $\overline{\mathbb{Q}}$. Soient S la surface de Riemann de $\mathcal{C}$, $(C_j)_{1\leq j\leq g}$ une base de son homologie en dimension 1, et $(\xi_h)_{1\leq h\leq g}$ une base définie sur $\overline{\mathbb{Q}}$ de l'espace des formes différentielles de première espèce sur S . Pour $1 \leq j \leq 2g$, on pose $\omega_j = (\omega_{1,j}, \ldots, \omega_{g,j}) \in \mathbb{C}^g$ où

$$\omega_{h,j} = \int_{C_j} \xi_h \ , \ (1 \leq h \leq g) \quad .$$

Soit $A = \mathbb{C}^g/\Omega$ la jacobienne de $\mathcal{C}$, où $\Omega = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_{2g}$. En appliquant le théorème 2.1 à un homomorphisme analytique $\mathbb{C}^g \to \mathbb{C} \times A_{\mathbb{C}}$ de la forme

$$(z_1,\ldots,z_g) \longmapsto (z_h \ , \Theta(z_1,\ldots,z_g))$$

avec $1 \leq h \leq g$, et où Θ est une représentation normalisée de l'exponentielle de A , on en déduit que pour $1 \leq h \leq g$, l'un des nombres $\omega_{h,1},\ldots,\omega_{h,2g}$ est transcendant.

Quand on applique ce résultat à une courbe de Fermat $x^N + y^N = 1$, on obtient la transcendance des nombres $B(a,b)$, quand a,b sont des nombres rationnels non entiers.

Ces résultats de Schneider peuvent être rendus effectifs : au lieu de montrer seulement que $P(B(a,b)) \neq 0$ quand $P(x) \in \mathbb{Z}[x]$ est un polynôme non nul, on peut minorer $|P(B(a,b))|$ en fonction de la hauteur et du degré de P. Il revient au même de minorer $|B(a,b) - \beta|$ quand β est un nombre algébrique. Le résultat suivant est dû à M. Laurent.

Théorème 4.1 : Soient r,s,N trois entiers naturels premiers entre eux dans leur ensemble. On suppose que ni r, ni s n'est divisible par N. Il existe un nombre $C > 0$ effectivement calculable en fonction de r,s,N, tel que pour tout nombre algébrique β de hauteur $\leq B$ (avec $B \geq 16$) et de degré $\leq D$ on ait

$$|B(\tfrac{r}{N},\tfrac{s}{N}) - \beta| \geq \exp\{-C\, D^n\, (\log H)\, (\log\log H)^n\}$$

où $\log H = \log B + D \log D$ et $n = \max\{1, \varphi(N)/2\}$.

Pour les nombres transcendants liés aux courbes elliptiques, E. Reyssat a donné une liste très complète de mesures de transcendance [7]. Ainsi le nombre ω/π a un type de transcendance $< 2+\varepsilon$ pour tout $\varepsilon>0$, et si α est un nombre algébrique non nul, $\wp(\alpha)$ n'est pas un U-nombre.

Enfin une version effective du théorème de Schneider sur la transcendance de l'invariant modulaire $j(\tau)$ (pour τ algébrique non imaginaire quadratique) a été obtenue récemment par D. Brownawell et D.W. Masser.

§5. Indépendance algébrique

L'étude de l'indépendance algébrique de nombres liés aux fonctions elliptiques a été beaucoup développée depuis le travail de Brownawell et Kubota en 1975. Les progrès les plus remarquables sont dus à G.V. Choodnovsky [2], dont voici deux résultats.

Théorème 5.1 : Soit $\wp$ une fonction elliptique de Weierstrass, d'invariants g_2, g_3 algébriques.

a) Soient ω une période de $\wp$, et u un point algébrique de $\wp$ (i.e. une période de $\wp$, ou bien un point où $\wp$ prend une valeur algébrique). On suppose u et ω linéairement indépendants sur $\mathbb{Q}$.

Alors les deux nombres

$$\zeta(u) - \frac{\eta}{\omega}u \ , \ \frac{\eta}{\omega}$$

sont algébriquement indépendants.

b) Si u_1, u_2 sont deux points algébriques de $\wp$ linéairement indépendants sur $\mathbb{Q}$, deux des nombres

$$u_1, u_2 \ , \ \zeta(u_1) \ , \ \zeta(u_2)$$

sont algébriquement indépendants.

Un résultat similaire au théorème 5.1.b., mais plus faible, a été obtenu par P. Philippon [6] dans le cas ultramétrique : soit p un nombre premier, $\wp_p$ une fonction elliptique de Weil-Lutz d'invariants g_2, g_3 algébriques, et ζ_p la primitive impaire de $-\wp_p$ (ces fonctions sont définies sur un idéal $\mathcal{D}_p$ du complété de la clôture algébrique du corps $\mathbb{Q}_p$). Si u_1, u_2, u_3 sont des éléments de $\mathcal{D}_p$ linéairement indépendants sur $\mathbb{Q}$, où la fonction $\wp_p$ prend des valeurs algébriques, alors, deux des nombres

$$u_1, u_2, u_3, \zeta_p(u_1), \zeta_p(u_2), \zeta_p(u_3)$$

sont algébriquement indépendants.

En l'abscence d'un bon "lemme de zéros" p-adique, Philippon est amené à utiliser le résultat d'analyse complexe suivant, qu'il démontre en généralisant un argument de Masser.

Proposition 5.2 : Soient Λ un réseau de Riemann de $\mathbb{C}^n$, $f_1, \dots, f_n$ n fonctions abéliennes par rapport à Λ, $g_1, \dots, g_{2n}$ $2n$ fonctions pseudo-périodiques par rapport à Λ, et θ une fonction théta associée à Λ, telle que $\theta f_1, \dots, \theta f_n$, $\theta g_1, \dots, \theta g_{2n}$ soient entières. Soit d'autre part P un élément de $\mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_{2n}]$ de degrés en $X_1, \dots, X_n$ (resp. $Y_1, \dots, Y_{2n}$) majorés par L_X (resp. L_Y). Alors, la fonction entière

$$\Phi(z) = (\theta(z))^{n(L_X+2L_Y)} P(f_1(z), \dots, f_n(z), g_1(z), \dots, g_{2n}(z))$$

est identiquement nulle, ou vérifie, pour tout nombre réel $R \geq 0$:

$$\Theta(\Phi, R) \leq c(L_X+L_Y)(L_Y^2+R^2) ;$$

dans cette inégalité, c désigne un nombre réel indépendant de P et de R, et $\Theta(\Phi, R)$ est la masse moyenne de la fonction Φ sur la boule de rayon R.

Enfin, E. Reyssat vient d'obtenir le résultat suivant.

Théorème 5.3 : Soient $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, et ζ la fonction zêta associée à $\wp$. Soient ω, ω' deux périodes de $\wp$ linéairement indépendantes sur $\mathbb{Q}$; on note $\tau = \omega'/\omega$, et η la quasi-période de ζ associée à ω . Soient u,v deux nombres complexes dont aucun multiple rationnel n'est période de $\wp$, et dont la différence n'est pas période de $\wp$. On définit enfin la fonction

$$f_{u,\omega}(z) = \frac{\sigma(z-u)}{\sigma(z)\ \sigma(u)}\ e^{zu\eta/\omega}$$

Alors :

a) parmi les cinq nombres

$$\wp(u)\ ,\ \wp(v)\ ,\ \zeta(u) - \frac{\eta}{\omega}\,u\ ,\ e^{i\pi u/\omega}\ ,\ f_{u,\omega}(v)\ ,$$

deux au moins sont algébriquement indépendants

b) parmi les dix nombres

$$\frac{\pi}{\omega}\ ,\ \frac{\eta}{\omega}\ ,\ \wp(u)\ ,\ \wp(v)\ ,\ \zeta(u)-\frac{\eta}{\omega}u\ ,\ \zeta(v)-\frac{\eta}{\omega}v\ ,\ e^{i\pi\tau}\ ,\ e^{i\pi u/\omega}\ ,\ e^{i\pi v/\omega}\ ,\ f_{u,\omega}(v),$$

trois au moins sont algébriquement indépendants.

En considérant la fonction $s(z) = \sigma(z)\ e^{-z^2\eta/2\omega}$, il en déduit en particulier :

Corollaire 5.4 : Sous les hypothèses du théorème, et si $\wp(u)$ est algébrique alors

a) Deux des trois nombres

$$e^{i\pi u/\omega}\ ,\ s(u)\ ,\ s'(u)$$

sont algébriquement indépendants.

b) Trois des six nombres

$$\frac{\pi}{\omega}\ ,\ \frac{\eta}{\omega}\ ,\ e^{i\pi\tau}\ ,\ e^{i\pi u/\omega}\ ,\ s(u)\ ,\ s'(u)$$

sont algébriquement indépendants.

§6. Plusieurs variables

Après une suggestion de Nagata et un mémoire de Bombieri en 1970, il est apparu important d'étudier les degrés des hypersurfaces algébriques ayant des singularités données.

Si S est un sous-ensemble fini de $\mathbb{C}^n$ et t un entier positif, on note $\omega_t(S)$ le plus petit des degrés des hypersurfaces algébriques ayant en chaque point de S une singularité d'ordre $\geq t$. Ce nombre $\omega_t(S)$ permet de généraliser à plusieurs variables des énoncés en une variable faisant intervenir le nombre $t \operatorname{card} S$ (cf. [8]). En voici un exemple, dû à J.C. Moreau [5].

Théorème 6.1 : Soient S un sous-ensemble fini de $\mathbb{C}^n$, et t un entier positif ; il existe un nombre réel $r_o = r_o(S,t)$ tel que si f est une fonction entière ayant en chaque point de S un zéro d'ordre $\geq t$, on ait pour $R \geq r > r_o$:

$$\operatorname{Log} |f|_r \leq \operatorname{Log} |f|_R - \omega_t(S) \operatorname{Log} \frac{R}{e^n r} .$$

En utilisant un résultat de [8], J.C. Moreau [5] en déduit qu'on peut remplacer $r_o(S,t)$ par $r_1(S,\varepsilon)$ (indépendant de t, avec $\varepsilon > 0$ arbitraire), pourvu que l'on remplace $\omega_t(S)$ par $\omega_t(S) - t\varepsilon$.

Ces nombres $\omega_t(S)$ interviennent dans la construction, due à Nagata, d'un contre exemple au quatorzième problème de Hilbert.

Références

[1] BERTRAND (Daniel).- Sur les périodes de formes modulaires ; C. r. Acad. Sci., Paris, t. 288, 1979, pp. 531-534.

[2] CHOODNOVSKY (Gregory V.).- Algebraic independence of values of exponential and elliptic functions ; Proc. I.C.M., Helsinki (1978).

[3] GROSCOT (Herbert).- Points entiers sur les courbes elliptiques ; Thèse de troisième cycle (Paris VI), 1979.

TRAVAUX RĒCENTS

[4] LAURENT (Michel).- Transcendance de périodes d'intégrales elliptiques ; J. für reine u. angew. Math., à paraitre.

[5] MOREAU (Jean-Charles).- Lemmes de Schwarz à plusieurs variables ; Séminaire d'Analyse (P. LELONG, H. SKODA), 1978-79, Lecture Notes in Math. (Springer Verlag) 1980.

[6] PHILIPPON (Patrice).- Indépendance algébrique de valeurs de fonctions elliptiques p-adiques, Preprint Ecole Polytechnique M436.0979, 1979.

[7] REYSSAT (Eric).- Approximation algébrique de nombres liés aux fonctions elliptiques et exponentielle ; Bull. Soc. Math. France, à paraitre .

[8] WALDSCHMIDT (Michel).- Nombres transcendants et groupes algébriques, Astérisque (S.M.F.) 69-70 (1979).

D. Bertrand
Ecole Polytechnique
Centre de Mathématiques
91128 Palaiseau Cedex

M. Waldschmidt
Université P. et M. Curie
Mathématiques, T.45-46
75230 Paris Cedex 05