BULLETIN DE LA S. M. F.

D.W. MASSER

Specialization of endomorphism rings of abelian varieties

Bulletin de la S. M. F., tome 124, nº 3 (1996), p. 457-476

<http://www.numdam.org/item?id=BSMF_1996__124_3_457_0>

Bull. Soc. math. France,
124, 1996, p. 457–476.

SPECIALIZATIONS OF ENDOMORPHISM RINGS OF ABELIAN VARIETIES

BY

D.W. MASSER

ABSTRACT. — Let k be a number field with algebraic closure $\bar{k}$, let V be a variety defined over k, and let A be an abelian variety defined over the function field $k(V)$. It is shown that for v in $V(\bar{k})$ the absolute endomorphism ring $\operatorname{End} A_v$ of the «fibre» A_v is «almost always» isomorphic to the absolute endomorphism ring $\operatorname{End} A$; and even that the «exceptional set» of such v, where there is no such isomorphism, is «sparse». More precisely, fix a projective embedding φ of V over k and let h_φ be the associated absolute logarithmic Weil height. Then there is a constant λ, depending only on the dimension of A, and a constant C, depending only on k, V, A and φ, with the following property. For any real $d \geq 1$ and $h \geq 1$ there exists a homogeneous polynomial of degree at most $C(\max\{d,h\})^\lambda$, not vanishing identically on V, that vanishes at all exceptional v in $V(\bar{k})$ with $[k(v):k] \leq d$ and $h_\varphi(v) \leq h$. For example, this implies that for any real $H \geq 3$ there are at most $C(\log H)^\lambda$ positive integers $v \leq H$ for which the Jacobian of the curve $y^5 = x(x-1)(x-v)$ has complex multiplication; or, there are at most $CH^5(\log H)^\lambda$ sets of positive integers $v_0, \ldots, v_5 \leq H$ for which the Jacobian of the curve $y^2 = v_0x^5 + \cdots + v_5$ has non-trivial endomorphisms.

The proofs involve recent estimates of Wüstholz and the author [Math. Z. 215, 1994, p. 641–653] for generators of endomorphism rings, together with an inequality of Lange and some effective elimination techniques using zero estimates from transcendence theory and Wronskians.

RÉSUMÉ. — Soient k un corps de nombres, $\bar{k}$ une clôture algébrique de k, V une variété définie sur k et A une variété abélienne définie sur le corps de fonctions $k(V)$. On montre que, si v appartient à $V(\bar{k})$, l'anneau d'endomorphisme absolu $\operatorname{End} A_v$ de la «fibre» A_v est «presque toujours» isomorphe à l'anneau d'endomorphisme absolu $\operatorname{End} A$; en fait, «l'ensemble exceptionnel» des v pour lesquels cela n'a pas lieu est «peu dense». Plus précisément, soient φ un plongement projectif de V et h_φ la hauteur de Weil logarithmique absolue associée. Il existe alors une constante λ, ne dépendant que de la dimension de A, et une constante C, ne dépendant que de k, V, A et φ satisfaisant à la condition suivante: si d et h sont deux réels ≥ 1, il existe un polynôme homogène de degré au plus $C(\max\{d,h\})^\lambda$, non identiquement nul sur V, qui s'annule en tout point exceptionnel v dans $V(\bar{k})$ tel que $[k(v):k] \leq d$ et $h_\varphi(v) \leq h$. Cela

(*) Texte recu le 26 avril 95, révisé le 17 juillet 1995.

D.W. MASSER, Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland. Email: masser@math.unibas.ch.

AMS classification: 14K, 11G, 11J.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037–9484/1996/457/$ 5

implique par exemple que, pour tout réel $H \geq 3$, il existe au plus $C(\log H)^{\lambda}$ entiers positifs $v \leq H$ tels que la jacobienne de la courbe $y^5 = x(x-1)(x-v)$ admette de la multiplication complexe; ou bien, qu'il y a au plus $CH^5(\log H)^{\lambda}$ familles d'entiers positifs $v_0, \ldots, v_5 \leq H$ telle que la jacobienne de la courbe $y^2 = v_0x^5 + \cdots + v_5$ admette un endomorphisme non trivial.

Les démonstrations font appels à des estimations, obtenues récemment par Wüstholz et l'auteur [Math. Z. 215, 1994, p. 641–653], sur les générateurs des anneaux d'endomorphismes, ainsi qu'à une inégalité de Lange et à des techniques d'élimination effective (« zero estimates » et wronskiens).

1. Introduction

Over the field $\mathbb{C}$ of complex numbers, it is well-known, and easy to prove, that « almost all » abelian varieties are simple, and even that they have trivial endomorphism rings consisting only of multiplications by the ring $\mathbb{Z}$ of rational integers. For example, this may be interpreted in measure-theoretical terms on some appropriate moduli space. Alternatively one can use notions of algebraic independence; such a point of view was considerably developed by Shimura in an important paper [Sh] (see in particular his section 4).

Over the field $\overline{\mathbb{Q}}$ of algebraic numbers, or over a fixed number field, one may expect a similar situation, although it is not so easy even to interpret the sense of « almost all » in this case. In the present paper we prove precise versions of such statements, in somewhat generalized form, and we give a number of illustrations. One of these, for instance, shows that the recent counterexamples to a conjecture of Coleman, constructed by de Jong and Noot [JN], are « sparse ». We have already in [Ma3] applied our results to the study of « large period matrices »; these are of interest in connexion with recent work of David [D] on a conjecture of Lang.

Our viewpoint will be similar to that taken in a previous paper [Ma2] on specializations of Mordell-Weil groups. Namely, let k be a subfield of $\mathbb{C}$, let V be a variety defined over k, and let A be an abelian variety defined over the function field $k(V)$. We may also think of this as a family of abelian varieties parametrized by points of V. More precisely, after replacing V by a non-empty open subset if necessary (an operation frequently to be performed in this paper), we may suppose that for each v in $V(\mathbb{C})$ the corresponding specialization from $k(V)$ to $k(v)$ provides an abelian variety A_v defined over $k(v)$ in $\mathbb{C}$.

We now have a « generic » endomorphism ring End A consisting of all endomorphisms of A. These might be defined over a finite extension of $k(V)$, rather than over $k(V)$ itself. For greater generality we do not assume that this endomorphism ring is trivial. Also for each v in $V(\mathbb{C})$ we have the « special » endomorphism ring End A_v consisting of all endomorphisms defined over $\mathbb{C}$. We shall say that v in $V(\mathbb{C})$ is exceptional if the rings End A_v and End A are not isomorphic.

As implied above, our interest lies mainly in the number field case, so from now on we shall assume that k is a number field with algebraic closure $\bar{k}$ embedded in $\mathbb{C}$. We wish to prove that the exceptional points of $V(\bar{k})$ are scarce. We measure this as in [Ma2] by fixing an affine embedding of V over k and then using the corresponding (absolute logarithmic) Weil height function to define an arithmetic filtration of these exceptional points in $V(\bar{k})$. Namely, for real numbers $d \geq 1$, $h \geq 1$ we define

$$v_{\mathrm{ex}}(d,h) = v_{\mathrm{ex}}(k;d,h)$$

to be the set of exceptional points v of

$$[k(v):\mathbb{Q}] \leq d, \quad h(v) \leq h. \tag{1.1}$$

Elementary height considerations show this to be finite. Accordingly for any finite subset S of $V(\mathbb{C})$ we write $\omega(S) = \omega_V(S)$ for the least degree of any polynomial that vanishes on S but not identically on V. Our main result can now be stated as follows.

THEOREM. — *Let k,V,A be as above, and suppose A has dimension $n \geq 1$. Then there exists C, depending only on V and A, and there exists λ, depending only on n, such that*

$$\omega\big(V_{\mathrm{ex}}(d,h)\big) \leq C\big(\max\{d,h\}\big)^{\lambda}$$

for all $d \geq 1$ and $h \geq 1$.

By way of comparison, note that if we consider the full set $V(d,h)$ of elements v of $V(\bar{k})$ satisfying (1.1), then Scholium 1, p. 414, of [Ma2] implies that

$$\omega\big(V(d,h)\big) > \exp(ch) \tag{1.2}$$

for suitable d and some $c > 0$ independent of h; in fact it suffices to take d as the degree of V in the given embedding. Thus the exceptional sets $V_{\mathrm{ex}}(d,h)$ grow «logarithmically slowly» compared to the full sets $V(d,h)$, at least with respect to the parameter h.

We shall give several examples for our theorem later on in section 6, but here we mention just two.

Firstly, it was the curves of genus 4 defined by

$$y^5 = x(x-1)(x-v)$$

that were considered by de Jong and Noot [JN]; they proved for the Jacobians A_v that there are actually infinitely many exceptional points. Our theorem implies, for example, that for any $H \geq 3$ there are most $c(\log H)^{\lambda}$

non-negative integers $v \leq H$ such that $\operatorname{End} A_v$ is not the ring of integers of $\mathbb{Q}(\exp(2\pi i/5))$.

Second, for $v = (a_0, \ldots, a_5)$ let A_v be the Jacobian of the «universal hyperelliptic curve of genus 2» defined by

$$y^2 = a_0x^5 + \cdots + a_5.$$

Our result implies similarly that for each $H \geq 3$ there is a non-zero polynomial $P(X_0, \ldots, X_5)$, of degree at most $c(\log H)^\lambda$, such that $P(a_0, \ldots, a_5) = 0$ for all non-negative integers $a_0, \ldots, a_5 \leq H$ such that $\operatorname{End} A_v$ is not $\mathbb{Z}$. It follows from a simple counting argument that this happens for at most $cH^5(\log H)^\lambda$ such elements $v = (a_0, \ldots, a_5)$, compared with at least H^6 altogether.

It is interesting to compare our theorem with a result of André [A, p. 201]. On the one hand he places more restrictions on the family A; thus $n \geq 3$ should be odd, V should be a curve, A should be simple, and there is an additional hypothesis of multiplicative reduction which implies that the tensor product $\mathbb{Q} \otimes \operatorname{End} A$ embeds into the ring $M_n(\mathbb{Q})$ of square matrices of order n with entries in the field $\mathbb{Q}$ of rational numbers. On the other hand, now defining the (possibly smaller) exceptional set V_{exex} as the set of v for which $\mathbb{Q} \otimes \operatorname{End} A_v$ has no such embedding, he is able to prove that the cardinality of $V_{\text{exex}}(d, h)$ remains bounded as $h \to \infty$. This looks like a special case of our theorem «without h» , and it raises the question of whether or theorem itself might be true without h. That the answer to this question could sometimes lie rather deep is illustrated by some of the examples we give in section 6.

Actually, as André himself pointed out to me, his results can be combined with ours. When his result applies, it yields the inequality (see [A, p. 202])

$$h(v) \leq c\,d^\kappa \tag{1.3}$$

for all v in his exceptional set $V_{\text{exex}}(d, h)$, again for c independent of d and h, and κ depending only n. Using our theorem, we conclude (when V is a curve) that $V_{\text{exex}}(d, h)$ contains at most $c\,d^\mu$ points, independently of h, for $\mu = \lambda \max\{1, \kappa\}$; such an estimate does not follow from (1.3) alone, since the height is logarithmic. An example is provided by the Jacobians A_v of the curves of genus 3 defined by

$$y^2 = x(x-1)(x-v)(x-v^2)(x-v^4)(x-v^5)(x-v^8).$$

Thus for any $d \geq 1$ there are at most cd^μ algebraic numbers v of degree at most d for which A_v is of simple CM type. But a full proof of this assertion must be deferred to a later paper.

The results of André are proved using the method of G-functions in the general context of transcendence theory. The proof of our theorem also ultimately rests on transcendence. The key tool is an estimate for endomorphisms established by Wüstholz and the author in [MW3], as a consequence of the main result of [MW2] proved using Baker's method. This is applied in section 2 to obtain a relation (Lemma 2.1) between the sets $V_{\mathrm{ex}}(d,h)$ and certain other sets $V_{\mathrm{ex}}(t)$ defined by a second, purely geometric filtration. After this, there is no more number theory, and our proposition, also stated in section 2, gives an upper bound for $\omega(V_{\mathrm{ex}}(t))$ in terms of the parameter t. The proof is essentially an extended exercise in effective elimination estimates, and it occupies sections 3, 4 and 5. We also record in section 2 a consequence of the sharp effective form of the Hilbert nullstellensatz established first by Brownawell.

In section 3 we introduce coordinates on the abelian varieties A_v and we use a result of Lange to estimate the degrees of equations defining endomorphisms. We then make the coordinates into abelian functions by introducing derivations, and for these we record a «zero estimate» of a kind familiar in the context of transcendence theory.

In section 4 we construct certain systems of auxiliary polynomials whose purpose is to «encode» the generic endomorphism ring $\mathrm{End}\, A$, which we identify with $\mathrm{End}\, A_\eta$ for a generic point η of V. The encoding is *via* analytic representations, and relies on generalized Wronskians together with the zero estimate of section 3.

In section 5 we use the effective nullstellensatz to reformulate this encoding property in terms of a system of polynomial identities over $\mathbb{C}$. We then «refine» these identities so that they are defined over the field $k(\eta)$. Roughly speaking, they thus involve a denominator $Q(\eta)$ in the ring $k[\eta]$. Now the proposition can be proved by observing that if v is an exceptional point then the above «encoding» must break down for $\mathrm{End}\, A_v$. This can happen essentially only if $Q(v) = 0$, which provides our estimate for ω.

Finally in section 6 we give the details for our examples.

When I first talked about these results in Paris, Daniel Bertrand raised the interesting question of what kind of estimates for the exceptional sets could be obtained using Hilbert's irreducibility theorem. He sketched an argument in the case $d = 1$, based on specialization properties of ℓ-adic Galois representations, suggesting that the set $V_{\mathrm{ex}}(k)$ of exceptional points over k is a «thin set» in $V(k)$ in the sense of Serre [Se2, p. 121]. Later on I learnt from Rutger Noot that the Galois representation properties had been proved by Serre himself in a letter [Se1] to Ribet. The details can be found, together with the application to endomorphisms (and Mumford-

Tate groups, among other things), in a preprint by Noot [No], and this work does indeed imply that $V_{\mathrm{ex}}(k)$ is a thin set.

If V is a curve, one can deduce estimates for the sets $V_{\mathrm{ex}}(1,h)$ in this way. For there are essentially best possible estimates for thin sets (see for example [Se2, pp. 132-136]) which are «often», but not always, polynomial in the logarithmic height h. For higher-dimensional V there are also cardinality estimates [Se2, Thms. 3 and 4, p. 178], but these seem not to be best possible unless one restricts to «integer points» [Se2, Thms. 1 and 2, pp. 177–178]. In any case it is not clear how they can lead to our polynomial estimates for ω. For example, if S is a thin subset of $\mathbb{Z}^m$ in affine space $V = \mathbb{A}^m$, a cardinality estimate of order H^ν for points of S with height at most $h = \log H$ would lead to an estimate for ω of order $H^{\nu/m}$. We can get any $\nu > m - \frac{1}{2}$ in general, and perhaps any $\nu > m - 1$ «often», but neither of the resulting estimates for ω can be polynomial in h if $m \geq 2$.

The situation gets worse if we consider the sets $V_{\mathrm{ex}}(d,h)$ for fixed $d > 1$. In fact there do not seem to be any analogous estimates at all in the literature for thin sets. Even if there were, they could not possibly be polynomial in h. For example, a typical thin set in $\bar{k}$ arises, from a polynomial $P(Y,X)$ in $k[Y,X]$ irreducible over $k(Y)$, as the set of v such that $P(v,X)$ is reducible over $k(v)$. But this happens in particular for all v such that $P(v,X) = 0$ for some x in k. These v have bounded degree, and it easily seen that their number with logarithmic height at most h grows at least exponentially in h (compare (1.2) above).

Incidentally, all these remarks apply equally to the exceptional sets discussed in [Ma2] in connexion with Mordell-Weil groups; that these are thin sets was proved by Néron (see also [Se2, p. 152]).

Various versions of this article were written up at various times in ETH Zürich and MPI Bonn, and I am grateful to both institutions for their hospitality and support. I also thank Y. André, R. Noot, Y. Zarhin and especially D. Bertrand for valuable conversations.

2. Preliminaries

We first observe that it suffices to prove our theorem when $A/k(V)$ is what might be called «endomorphism-stable», that is, all endomorphisms of A are already defined over $k(V)$. For in general they are defined over some finite extension K of $k(V)$, which we can write as $k'(V')$ for some covering V' of V defined over a finite extension k' of k. We can now consider A as a family A' over $k'(V')$, and as such it is clearly endomorphism-stable. Suppose now that v lies in the exceptional set in V.

Then any v' in V' over v lies in the exceptional set in V'. Further if v is in $V_{\text{ex}}(d,h)$ then standard height estimates (see for example [Ma2, p. 419]) show that v' lies in $V'_{\text{ex}}(c\,d, c\,h)$ for some c independent of d and h. So the theorem for A' over $k'(V')$ provides a polynomial vanishing at all such v'. Now taking norms and clearing denominators leads to a polynomial vanishing at all v, and standard estimates for these procedures lead to a proof of the general theorem for A over $k(V)$.

In a similar way we may extend the coordinate ring $k[V]$ of V to include any finite set of fixed elements of $k(V)$. More generally we may replace V by a non-empty open subset, or equivalently restrict our attention to « almost all » v; these operations change the counting function ω additively by only a bounded amount, and we shall employ them frequently during the subsequent arguments.

The technical convenience of endomorphism-stability is that in this case we have a unique specialization homomorphism σ_v from $\operatorname{End} A$ to $\operatorname{End} A_v$, at least for all v in a non-empty open subset of V. Henceforth we shall assume that this is indeed the case, and we write $K = k(V)$. We shall establish our theorem by proving that σ_v is very often an isomorphism.

It is rather easy to prove that σ_v is almost always injective. Let Tr be the trace function from $\operatorname{End} A$ to $\mathbb{Z}$, normalized so that $\operatorname{Tr}(1) = 2n$. It is well-known that the bilinear form defined by $\operatorname{Tr}(fg)$ is non-degenerate. Thus if $f_1, \dots, f_\ell$ are basis elements of $\operatorname{End} A$, the determinant $\det \operatorname{Tr}(f_i f_j)$ $(1 \leq i, j \leq \ell)$ is non-zero. But traces are unchanged under specialization, as we see from considering regular representations. It follows that $\det \operatorname{Tr}(\sigma_v(f_i)\sigma_v(f_j))$ is also non-zero, and so $\sigma_v(f_1), \dots, \sigma_v(f_\ell)$ are independent in $\operatorname{End} A_v$. Therefore σ_v is an injection.

So the study of exceptional points is reduced to a problem of surjectivity, and to deal with this we will need a positive definite bilinear form. Thus let $\mathcal{D}$ be a very ample divisor on A defined over K, whose support does not contain the origin. It will be convenient later also to assume that $\mathcal{D}$ is three times an ample divisor. For almost all v this specializes to a very ample divisor $\mathcal{D}_v$ on A_v, and we have a Rosati involution i_v on $\mathbb{Q} \otimes \operatorname{End} A_v$ and a corresponding bilinear form $t_v(f,g) = \operatorname{Tr}(i_v(f)g)$. We put $t_v(f) = t_v(f,f)$ as usual.

We introduce a second filtration on the set V_{ex} of exceptional points as follows. For a real number $t \geq 1$ we define $V_{\text{ex}}(t)$ as the set of all v in $V(\bar{k})$ for which there exists f in $\operatorname{End} A_v$, not in $\sigma_v(\operatorname{End} A)$, with $t_v(f) \leq t$. The relation between the two filtrations is contained in the following result. For the rest of this paper, c will denote an unspecified sufficiently large positive constant, not necessarily the same at each occurrence, that depends only on V and A (and the divisor $\mathcal{D}$).

LEMMA 2.1. — *There exists τ, depending only on n, such that for every $d \geq 1$ and $h \geq 1$ the set $V_{\mathrm{ex}}(d,h)$ is contained in $V_{\mathrm{ex}}(t)$ for some t not exceeding $c(\max\{d,h\})^{\tau}$.*

Proof. — For $d \geq 1$ and $h \geq 1$ let v be in the exceptional set $V_{\mathrm{ex}}(d,h)$. By Lemma 2.1, p. 414, of [MW2], all elements of $\mathrm{End}\, A_v$ are defined over an extension field k' of $k(v)$ of relative degree at most c. By Lemma 5.1, p. 651, of [MW3] applied to the fibre A_v over k', the additive group $\mathrm{End}\, A_v$ has basis elements $f_1, \dots, f_\ell$ satisfying

$$t_v(f_i) \leq c\big(\max\{d, h(A_v)\}\big)^{\tau} \qquad (1 \leq i \leq \ell),$$

where $h(A_v)$ is the (absolute logarithmic semistable) Faltings height of A_v, and τ depends only on n. It is not difficult to prove that $h(A_v) \leq c\,h$ (see for example the argument in the proof of Lemma 2.2 of [Ma3], p. 160). It follows that

$$t_v(f_i) \leq c\big(\max\{d, h\}\big)^{\tau} \qquad (1 \leq i \leq \ell). \tag{2.1}$$

Now by hypothesis $\mathrm{End}\, A_v$ is strictly bigger than $\sigma_v(\mathrm{End}\, A)$, and it follows that $f = f_i$ is not in $\sigma_v(\mathrm{End}\, A)$ for some i with $1 \leq i \leq \ell$. Therefore v is in $V_{\mathrm{ex}}(t)$ where t is the right-hand side of (2.1). This proves the lemma.

Unfortunately the exponent τ is rather large; in fact

$$\tau = 4n(2n-1)q(2nq+1)^{n-1},$$

where $q = (p-1)4^p p!$ and $p = n(2n+1)$.

So for the proof of our theorem it remains only to bound the quantities $\omega(V_{\mathrm{ex}}(t))$ in a suitable way. This we do as follows.

PROPOSITION. — *There exists μ, depending only on n, such that $\omega(V_{\mathrm{ex}}(t)) \leq c\,t^{\mu}$ for every $t \geq 1$.*

Most of the rest of this paper is devoted to a proof of this proposition. We will actually prove it for any subfield k of $\mathbb{C}$, and thus from now on we can forget about number theory. But no generality is lost in assuming that k has finite transcendence degree; this is convenient when we use the language of generic points later on in section 3.

We finish the present section with a couple of observations on polynomials.

First, we will require the following simple remark about linear equations; it is the quantity r that will eventually provide our polynomial vanishing on $V_{\mathrm{ex}}(t)$.

LEMMA 2.2. — *Let $\mathcal{L}$ be a finite set of linear forms with coefficients in a subring $\mathcal{R}$ of $\mathbb{C}$ containing* 1. *Then there is a complex number $r \neq 0$ in $\mathcal{R}$, which is either* 1 *or a minor of the matrix of coefficients of $\mathcal{L}$, with the following property. Suppose that for each L in $\mathcal{L}$ there is λ_L in $\mathcal{R}$ such that the equations $L = \lambda_L$ (L in $\mathcal{L}$) have a solution over $\mathbb{C}$. Then they have a solution over $r^{-1}\mathcal{R}$.*

Proof. — If every form in $\mathcal{L}$ is zero the lemma is trivially true with $r = 1$. Otherwise their rank is $m \geq 1$, and by restricting to a maximal linearly independent subset, we see that r can be taken as any non-zero minor of order m. This completes the proof.

For a point $u = (u_1, \ldots, u_m)$ in $\mathbb{C}^m$ let $\mathcal{M}_u$ be the maximal ideal in the polynomial ring $\mathbb{C}[X_1, \ldots, X_m]$ with the generators $X_1 - u_1, ..., X_m - u_m$. For a finite subset U of $\mathbb{C}^m$ the product ideal of all the $\mathcal{M}_u$(u in U) has a set of standard generators obtained by taking products of the generators of the $\mathcal{M}_u$; this set we denote by $\mathcal{N}(U)$.

LEMMA 2.3. — *For a positive integer E let $\mathcal{P}$ be a finite set of polynomials in $\mathbb{C}[X_1,...,X_m]$, of degrees at most E, whose set S of common zeroes in $\mathbb{C}^m$ is countable. Then there is a finite subset U of S, of cardinality at most E^m, and a positive integer $e \leq 2(2E)^m$, such that for every N in $\mathcal{N}(U)$ we have*

$$N^e = \sum_{P \in \mathcal{P}} Q_{NP} P$$

for polynomials Q_{NP} in $\mathbb{C}[X_1,...,X_m]$ of degrees at most $2(2E)^{2m}$.

Proof. — Of course the countable algebraic set S is finite, and now the cardinality estimate for $U = S$ is well-known; one can use for example the Corollary, p. 419, of [MW1], or also Proposition 3.3, p. 365, of [P]. The estimates for e and the degrees of the Q_{NP} then follow immediately from the main result of [B] with $\mu \leq m$ and $D = E$, $D_0 \leq E^m$.

3. Functions and derivations

Let A be our abelian variety over the field $K = k(V)$. We shall require functions on A, and so we fix basis elements $x_1, \ldots, x_s$ of the linear system over K corresponding to the divisor $\mathcal{D}$. These are regular at the origin. Let $x = (x_1, \ldots, x_s)$ be the associated coordinate vector. By normality the coordinate ring of A corresponding to $\mathcal{D}$ is then $K[x] = K[x_1, \ldots, x_s]$.

All this specializes nicely, at least on a non-empty open subset of V, and so for v in $V(\mathbb{C})$ we shall write x_v for the coordinate vector on the abelian variety A_v. Let D be a positive integer. We shall say that an endomorphism f of A_v can be «rationally described by polynomials» of degree at most D if there are polynomials $P_0, P_1, \dots P_s$ in x_v, of degree at most D, such that f is given by $(P_1/P_0, \dots, P_s/P_0)$ on a non-empty open subset of A_v.

LEMMA 3.1. — *For v in $V(\mathbb{C})$ let f be a non-zero endomorphism of A_v. Then f can be "rationally described by polynomials of degree at most" $t_v(f)+1$.*

Proof. — Let $a_1, \dots, a_n$ be the eigenvalues of $i_v(f)f$ in the analytic representation. Then

$$\max\{a_1, \dots, a_n\} \leq a_1 + \cdots + a_n = \tfrac{1}{2} t_v(f) < m,$$

where m is the least integer exceeding $\frac{1}{2} t_v(f)$. We now apply Theorem 3.1, p. 618, of Lange [L]; this even tells us that f can be described as a morphism by forms of degree m on a union of open sets covering A_v, and so the proof is complete.

Fix basis elements, defined over K, of the tangent space of A at the origin. These are thus derivations from $K[x]$ to K. Using the group law, we can extend these in the usual way to invariant derivations $\partial_1, \dots, \partial_n$ from the function field $K(A) = K(x) = K(x_1, \dots, x_s)$ to itself. Because $K[x]$ is our coordinate ring, it follows that these also act on $K[x]$. By extending the coordinate ring of V, we can assume that these even act on $R[x]$ for $R = k[V]$.

All this too specializes nicely, at least on a non-empty open subset of V. Thus for all v in $V(\mathbb{C})$ we can regard the components of $x_v = x_v(z)$ as abelian functions of $z = (z_1, \dots, z_n)$ in $\mathbb{C}^n$. Here $\partial_1, \dots, \partial_n$ are identified with $\partial/\partial z_1, \dots, \partial/\partial z_n$; and these abelian functions satisfy polynomial partial differential equations over the ring $k[v]$.

For a positive integer T let $\Delta(T)$ be the set of derivations $\delta = \partial_1^{t_1} \cdots \partial_n^{t_n}$ of orders $t_1 + \cdots + t_n < T$. Let $M_n(\mathbb{C})$ be the ring of square matrices of order n with complex entries. Recall that the constants c depend only on V and A.

LEMMA 3.2. — *Suppose v is in $V(\mathbb{C})$ and u is in $M_n(\mathbb{C})$. For positive integers E and T let $\Phi(z)$ be a polynomial, with complex coefficients, of degree E in the components of $x_v(z)$ and $x_v(zu)$, such that $\delta\Phi(0) = 0$ for all δ in $\Delta(T)$. Then if $T > cE^{2n}$, the function $\Phi(z)$ vanishes identically.*

Proof. — We use zero estimates (from transcendence theory) on the algebraic group $G = A_v \times A_v$ and the analytic subgroup Z defined on the tangent space by $w = zu$. In particular, if $T \geq 4n$, then Théorème 2.1, p. 358, of [P] applied with $\Sigma = 0$, together with standard remarks about projective embeddings, leads to a connected algebraic subgroup H of G, with tangent space S, such that

$$(T'+1)\cdots(T'+m) \leq m!\, g(2E)^{2n}. \tag{3.1}$$

Here $T' = [T/(2n)] - 1$, g is the degree of G in the Segre embedding, and m is the codimension of the intersection of Z and S in Z. Further, the comments about translations in the Addendum to [P] (see also [Na]) imply that the polynomial associated with Φ vanishes on H. Now if c is large enough, our condition on T leads at once to $m = 0$ in (3.1), so that Z is contained in S, and therefore Φ itself vanishes identically. This completes the proof.

By once again extending the coordinate ring we can assume that the affine coordinates of the origin in A lie in the ring $R = k[V]$. The repeated effect of differentiating is then given as follows. For convenience we state the result in terms of generic points.

LEMMA 3.3. — *Let η be in $V(\mathbb{C})$ generic over k, and let α be in $M_n(\mathbb{C})$ generic over $k(\eta)$. For a positive integer E let $\Phi(z)$ be a polynomial, with coefficients in k and degree at most E, in either*

(a) *the components of η and $x_\eta(z)$, or*

(b) *the entries of α, and the components of η,$x_\eta(z)$ and $x_\eta(z\alpha)$.*

Then for any positive integer T and any δ in $\Delta(T)$ the function $\delta\Phi(z)$ is also a polynomial in the same quantities, with coefficients in k, of degree at most $E + cT$.

Proof. — There exists a positive integer c_0, depending only on V and A, such that each derivative $\partial_j x_{i\eta}(z)$ $(1 \leq j \leq n)$ of each coordinate $(1 \leq i \leq s)$ is a polynomial, with coefficients in k, of degree at most c_0 in the components of η and $x_\eta(z)$. So each $\partial_j x_{i\eta}(z\alpha)$ is a polynomial, with coefficients in k, of degree at most $c_0 + 1$ in the entries of α, and the components of η and $x_\eta(z)$. The desired result with $c = c_0$ now follows by a standard induction on T, and this completes the proof.

4. Wronskians

Let Y be variables on the ambient affine space of V, and let X be the standard affine variables on the matrix ring M_n. For each positive integer D and each positive integer T we will define certain subsets $\mathcal{I} = \mathcal{I}(D,T)$ of $k[Y]$ and $\mathcal{J} = \mathcal{J}(D,T)$ of $k[Y,X]$. The Wronskian determinant will play a crucial role in the construction, so we briefly review its definition and main properties.

For a complex variable $z = (z_1, \dots, z_n)$ let $\chi_1, \dots, \chi_m$ be functions holomorphic in some non-empty open subset of $\mathbb{C}^n$. Let $\delta_1, \dots, \delta_m$ be elements of the set $\Delta(m)$ defined in the previous section with reference to $\partial/\partial z_1, \dots, \partial/\partial z_n$. Then

$$W = W(\chi_1, \dots, \chi_m) = \det \delta_i \chi_j \qquad (1 \le i, j \le m)$$

is a (generalized) Wronskian of $\chi_1, \dots, \chi_m$. If $\chi_1, \dots, \chi_m$ are linearly dependent over $\mathbb{C}$ it is clear that $W = 0$; conversely, if $W = 0$ for all choices of $\delta_1, \dots, \delta_m$ then it is well-known that $\chi_1, \dots, \chi_m$ are linearly dependent over $\mathbb{C}$.

For convenience we work with a point η of $V(\mathbb{C})$ generic over k; the following constructions are easily seen to be independent of the choice of η. Let $x_\eta = (x_{1\eta}, \dots, x_{s\eta})$ be our affine coordinates on the abelian variety A_η. These are abelian functions $x_\eta(z)$ of the complex variable z. For a positive integer D let $H = H(D)$ be the maximum number of monomials of degree at most D in x_η that are linearly independent over $\mathbb{C}$ on A_η. Choose such monomials $M_1, \dots, M_H$ (for example minimal in some fixed lexicographic ordering) that are linearly independent on A_η. Consider the corresponding Wronskians

$$W(z) = W\big(M_1(x_\eta(z)), \dots, M_H(x_\eta(z))\big). \tag{4.1}$$

For a positive integer T and δ in $\Delta(T)$ it follows from Lemma 3.3 (a) that each $\delta W(0)$ is a polynomial over k in the components of η and $x_\eta(0)$, and therefore also in η alone. Denote by $\mathcal{I} = \mathcal{I}(D, T)$ a corresponding set of elements of $k[Y]$ (say of minimal degree) obtained in this way, as W and δ vary.

For v in $V(\mathbb{C})$ we write $\mathcal{I}(v) = 0$ if every element of $\mathcal{I}$ vanishes at v; and $\mathcal{I}(v) \neq 0$ otherwise.

LEMMA 4.1. — *The elements of $\mathcal{I}$ are polynomials over k of degrees at most $c(D^{2n} + T)$. Also*

(a) *if $\mathcal{I}(v) \neq 0$ for some v in $V(\mathbb{C})$, then $M_1(x_v(z)), \dots, M_H(x_v(z))$ are linearly independent over $\mathbb{C}$, and*

(b) *if further $T > cD^{4n^2}$, then $\mathcal{I}(\eta) \neq 0$.*

Proof. — By Theorem 1, p. 12, of [Ne] we have $H \le a(4D)^n$, where a is the projective degree of A_η. Thus $H \le cD^n$. By Lemma 3.3 (a) each $W(z)$ can be written as a polynomial over k of degree at most

$$E \le cH(D + H) \le cD^{2n} \tag{4.2}$$

in the components of η and $x_\eta(z)$. Again by Lemma 3.3 (a) each $\delta W(z)$ can be written as a polynomial over k of degree at most $c(E+T) \leq c(D^{2n}+T)$ in these components. The estimate for the degrees of the elements of $\mathcal{I}$ is immediate.

Next, if $\mathcal{I}(v) \neq 0$ for some v in $V(\mathbb{C})$, suppose to the contrary that $M_1(x_v(z)), \ldots, M_H(x_v(z))$ are linearly dependent over $\mathbb{C}$. Then every Wronskian of these functions vanishes, and therefore so does every derivative at the origin. Specializing the differential equations of Lemma 3.3 (a), we see that $\mathcal{I}(v) = 0$, a contradiction. This proves part (a) of the present lemma.

Finally suppose $\mathcal{I}(\eta) = 0$. Then for every W in (4.1) we have $\delta W(0) = 0$ for all δ in $\Delta(T)$. Since $W(z)$ is a complex polynomial in $x_\eta(z)$ of degree at most E, we see from Lemma 3.2 (without u) for $v = \eta$ that these imply $W(z) = 0$ provided $T > cE^{2n}$. By (4.2) this holds if $T > cD^{4n^2}$, and so we get the linear dependence of $M_1(x_\eta(z)), \ldots, M_H(x_\eta(z))$ over $\mathbb{C}$; however, this contradicts the definition of $M_1, \ldots, M_H$. So (b) is proved , and this establishes the present lemma.

LEMMA 4.2. — *Let D be a positive integer and let v be in $V(\mathbb{C})$. Then for any monomial M of degree at most D the functions $M_1(x_v(z)), \ldots,$ $M_H(x_v(z))$ and $M(x_v(z))$ are linearly dependent over $\mathbb{C}$.*

Proof. — Pick any positive integer T, and perform the above Wronskian construction with the monomials $M_1, \ldots, M_H$ and M instead of only $M_1, \ldots, M_H$. We get a subset $\mathcal{I}_M = \mathcal{I}_M(D,T)$ of $k[Y]$. However, the choice of $M_1, \ldots, M_H$ implies that $M_1(x_\eta(z)), \ldots, M_H(x_\eta(z))$ and $M(x_\eta(z))$ are linearly dependent over $\mathbb{C}$, and so this time all the elements of $\mathcal{I}_M$ must be zero at $Y = \eta$.

Therefore they are zero at $Y = v$, and this means that every Wronskian W of $M_1(x_v(z)), \ldots, M_H(x_v(z))$ and $M(x_v(z))$ satisfies $\delta W(0) = 0$ for all δ in $\Delta(T)$. Choosing $T > cD^{4n^2}$ and using again Lemma 3.2 as in the proof of the previous lemma, we see that this implies $W = 0$, and therefore the desired dependence relation. This completes the proof.

Probably a version of this lemma can be proved more directly using only the concept of flatness (see for example [H, pp. 261–262]). It would then hold for families of arbitrary varieties, not just abelian varieties. A similar remark applies to Lemma 4.1 (a). However, the machinery of Wronskians and zero estimates really does seem to be necessary in what follows.

For the construction of $\mathcal{J}$, let η be as above, and let α be a point of $M_n(\mathbb{C})$ generic over $k(\eta)$. This time, for each integer i with $1 \leq i \leq s$, we write down all Wronskians $W_i(z,\alpha)$ of the functions

$$M_1\big(x_\eta(z)\big), \ldots, M_H\big(x_\eta(z)\big), x_{i\eta}(z\alpha)M_1\big(x_\eta(z)\big), \ldots, x_{i\eta}(z\alpha)M_H\big(x_\eta(z)\big).$$

By Lemma 3.3 (b), for δ in $\Delta(T)$ the $\delta W_i(0,\alpha)$ are polynomials over k in the entries of α and the components of η. We write $\mathcal{J} = \mathcal{J}(D,T)$ for a corresponding set of elements of $k[Y,X]$ (again of minimal degrees) as i, W and δ vary.

To state the analogue of Lemma 4.1 we recall the definitions in section 3. Also our choice of derivations provides an analytic representation ρ from $\operatorname{End} A$ to $M_n(K)$. Since $\operatorname{End} A$ is finitely generated as an additive group, we can assume by extending the coordinate ring that ρ takes values in the ring $M_n(R)$ of matrices with entries in $R = k[V]$. By specialization we get for each v in $V(\mathbb{C})$ an analytic representation ρ_v from $\sigma_v(\operatorname{End} A)$ to the ring $M_n(k[v])$ of matrices with entries in $k[v]$. It extends to a representation, also denoted by ρ_v, from $\mathcal{E}_v = \operatorname{End} A_v$ to $M_n(\mathbb{C})$. Finally we use the analogous notation $\mathcal{J}(v,u) = 0$, $\mathcal{J}(v,u) \neq 0$ for v in $V(\mathbb{C})$ and u in $M_n(\mathbb{C})$.

LEMMA 4.3. — *The elements of $\mathcal{J}$ are polynomials over k of degrees at most $c(D^{2n} + T)$. Assume $T > cD^{4n^2}$. Then*

(a) *if $\mathcal{J}(\eta,u) = 0$ for some u in $M_n(\mathbb{C})$, then u is in $\rho_\eta(\mathcal{E}_\eta)$, and*

(b) *suppose $\mathcal{I}(v) \neq 0$ for some v in $V(\mathbb{C})$. If f in $\mathcal{E}_v$ can be rationally described by polynomials of degree at most D, then $\mathcal{J}(v,\rho_v(f)) = 0$.*

Proof. — The degree estimates are proved exactly as in Lemma 4.1, except that we use Lemma 3.3(b). We omit the details. As for (a) and (b), we assume $T > cD^{4n^2}$ from now on.

To begin with, suppose $\mathcal{J}(\eta, u) = 0$ for some u in $M_n(\mathbb{C})$. We deduce from an application of Lemma 3.2 (this time with u) for $v = \eta$ that the functions

$$M_1(x_\eta(z)),\ldots,M_H(x_\eta(z)),x_{i\eta}(zu)M_1(x_\eta(z)),\ldots,x_{i\eta}(zu)M_H(x_\eta(z))$$

are linearly dependent over $\mathbb{C}$ for each i with $1 \leq i \leq s$. Since the first H of these are independent, we deduce that each $x_{i\eta}(zu)$ $(1 \leq i \leq s)$ is a rational function of $x_\eta(z)$. It follows easily that these rational functions correspond to an endomorphism f of A_η, and that $u = \rho_\eta(f)$. This proves (a).

Next suppose $\mathcal{I}(v) \neq 0$ for some v in $V(\mathbb{C})$. Then Lemma 4.1 (a) together with Lemma 4.2 shows that every monomial of degree at most D in $x_v(z)$ is a linear combination of $M_1(x_v(z)),\ldots,M_H(x_v(z))$. If f in $\mathcal{E}_v$ can be rationally described by polynomials of degree at most D, it follows that with $u = \rho_v(f)$ each $x_{iv}(zu)$ $(1 \leq i \leq s)$ is a rational function of the $x_v(z)$ of degree at most D. We deduce that the functions

$$M_1(x_v(z)),\ldots,M_H(x_v(z)),x_{iv}(zu)M_1(x_v(z)),\ldots,x_{iv}(zu)M_H(x_v(z))$$

are linearly dependent. So every Wronskian vanishes, and it follows at once by differentiating and putting $z = 0$ that $\mathcal{J}(v,u) = 0$ as desired for (b). This completes the proof of the present lemma.

5. Identities

We proceed to translate Lemma 4.3 (a) into a system of polynomial identities. For a finite subset U of $M_n(\mathbb{C})$ recall the set $\mathcal{N}(U)$ of section 2, considered as a subset of the polynomial ring $\mathbb{C}[X]$. For positive integers D and T we write $P = P(Y,X)$ for the elements of $\mathcal{J} = \mathcal{J}(D,T)$.

LEMMA 5.1. — *Suppose $T > cD^{4n^2}$. Then there is a positive integer $e \leq cT^{n^2}$ and a subset U of $\rho_\eta(\mathcal{E}_\eta)$ of cardinality at most cT^{n^2}, such that for every N in $\mathcal{N}(U)$ we have*

$$\big(N(X)\big)^e = \sum_{P\in\mathcal{J}} Q_{NP}(X)P(\eta,X)$$

for polynomials $Q_{NP}(X)$ in $\mathbb{C}[X]$ of degrees at most cT^{2n^2}.

Proof. — From Lemma 4.3 (a), the polynomials $P(\eta,X)$ in $\mathbb{C}[X]$ have common zeroes only in the set $\rho_\eta(\mathcal{E}_\eta)$. This set is countable, and since by Lemma 4.3 the polynomials have degrees at most cT, the present lemma follows at once from Lemma 2.4.

The identities of Lemma 5.1 are defined over $\mathbb{C}$. We now proceed to refine them to a similar set of identities defined over the ring $k[\eta]$.

LEMMA 5.2. — *Suppose $T > cD^{4n^2}$, and let $\nu = 2n^4 + 1$. Then there is a polynomial $Q_0(Y)$ in $k[Y]$ of degree at most cT^ν, with $Q_0(\eta) \neq 0$, such that for every N in $\mathcal{N}(U)$ we have*

$$Q_0(\eta)\big(N(X)\big)^e = \sum_{P\in\mathcal{J}} \widetilde{Q}_{NP}(\eta,X)P(\eta,X)$$

for polynomials $\widetilde{Q}_{NP}(Y,X)$ in $k[Y,X]$.

Proof. — We regard the identities of Lemma 5.1 as linear equations for the coefficients of the polynomials $Q_{NP}(X)$. Naturally these equations are solvable over $\mathbb{C}$, and they are defined over the ring $k[\eta]$. By Lemma 2.2 there is therefore a solution over $r^{-1}k[\eta]$, where $r \neq 0$ is either 1 or a minor of the matrix of the homogeneous linear part of the equations. So $r = Q_0(\eta)$ for some $Q_0(Y)$ in $k[Y]$ (independent of N), and it remains only to estimate the degree of Q_0.

In the first place, both sides of the identities in Lemma 5.1 have degrees at most $D_0 \leq cT^{2n^2}$ in X. For each N there are therefore at most $D_1 = (D_0+1)^{n^2}$ linear equations to be solved. In each equation the coefficients of the homogeneous linear part are polynomials over k in η of degrees at most $D_2 \leq cT$, by Lemma 4.3. So we get for the minor $r = Q_0(\eta)$ a total degree in η not exceeding $D_1 D_2 \leq cT^{\nu}$ as claimed. This completes the proof.

We can now prove our proposition. We may assume that t is a positive integer. Let v be in the exceptional set $V_{\mathrm{ex}}(t)$. Thus there is f in $\mathcal{E}_v$, not in $\sigma_v(\mathcal{E}_\eta)$, with

$$(5.1) \qquad t_v(f) \leq t.$$

We choose $D = t+1$ and then

$$(5.2) \qquad T = c_0 D^{4n^2},$$

where c_0 is a positive integer, depending only on V and A, which is so large that the inequalities of Lemma 4.1, Lemma 4.3 and Lemma 5.2 hold.

We proceed to specialize the identities of Lemma 5.2 for $\mathcal{J} = \mathcal{J}(D,T)$ from the generic point η to the special point v. For this purpose the specialization homomorphism σ_v, which goes from $\mathcal{E}_\eta$ to $\mathcal{E}_v$, can also be regarded as a homomorphism from $k[\eta]$ to $k[v]$. Extending it to polynomials in X, we obtain for each N in $\mathcal{N}(U)$

$$(5.3) \qquad Q_0(v)\big(\sigma_v(N(X))\big)^e = \sum_{P\in\mathcal{J}} \widetilde{Q}_{NP}(v,X)P(v,X).$$

Assume for the moment that

$$(5.4) \qquad \mathcal{I}(v) \neq 0$$

for the set $\mathcal{I} = \mathcal{I}(D,T)$ of Lemma 4.1. By (5.1) and Lemma 3.1 the endomorphism f can be rationally described by polynomials of degree at most $D = t+1$. It follows from (5.4) and Lemma 4.3 (b) that the right-hand sides of (5.3) all vanish at $X = \rho_v(f)$. Hence, looking at the left-hand sides, we see that either

$$(5.5) \qquad Q_0(v) = 0$$

or all the $\sigma_v(N(X))$ vanish at $X = \rho_v(f)$.

Let us examine the second possibility more closely. The $\sigma_v(N)$ are the elements of the set $\mathcal{N}(\sigma_v(U))$, and therefore their common zeroes are contained in the set $\sigma_v(\rho_\eta(\mathcal{E}_\eta))$. Since the analytic representation specializes nicely, this latter set is just $\rho_v(\sigma_v(\mathcal{E}_\eta))$; however, this does not contain $\rho_v(f)$ by our hypothesis on f (note that ρ_v is faithful). Therefore this second possibility does not occur, and we have shown that either (5.5) holds or (5.4) does not.

But $\mathcal{I}(v) = 0$ means that every element of $\mathcal{I}$ in $k[Y]$ vanishes at v. By Lemma 4.1 (b) some element does not vanish at η, and this element can be written as $Q_1(Y)$ for some polynomial $Q_1(Y)$ in $k[Y]$ of degree at most cT.

Summing up, we have found a polynomial $Q = Q_0Q_1$ in $k[Y]$, not vanishing identically on the variety V, that vanishes at all v in $V_{\mathrm{ex}}(t)$. Therefore $\omega(V_{\mathrm{ex}}(t))$ is at most the degree of Q, which is at most $cT^{\nu+1}$. Recalling (5.2), we see that we have proved the proposition with exponent

$$\mu = 8n^2(n^4+1).$$

As we noted in section 2, the theorem follows immediately on combining this with Lemma 2.1, with exponent $\lambda = \mu\tau$.

6. Examples

From now on all the constants will be absolute. The simplest example is provided by the elliptic family over $\mathbb{Q}(\mathbb{A})$, the function field of affine space $\mathbb{A}$, defined by

$$y^2 = 4x^3 - gx - g, \qquad g = \frac{27j}{j-1728}.$$

The exceptional points correspond to quadratic values of the standard variable τ in the upper half plane, and the associated values $j = j(\tau) \neq 0, 1728$. Our theorem therefore implies that the number of such j with degree at most $d \geq 1$ and logarithmic height at most $h \geq 1$ is at most $c(\max\{d,h\})^\lambda$. Actually such an estimate, even with $\lambda = 6$, is a fairly immediate consequence of Lemma 3 (i), p. 187, of Faisant-Philibert [FP]. But of course both these results fall well short of what is known, and the classical theorems on class numbers of complex quadratic fields show that we can eliminate h in this estimate, which further supports the possibility raised in section 1.

Our next example refers to the paper [JN] of de Jong and Noot, where they give some families of counterexamples to a conjecture of Coleman. Our theorem can be used to show that their families do not contain many members. Thus let A_v be the Jacobian of the curve of genus 4 defined by

$$y^5 = x(x-1)(x-v).$$

They prove that A_v is simple and of CM type for infinitely many v in $\mathbb{C}$.

Now we have an associated family A over $k(\mathbb{A})$, where $k = \mathbb{Q}(\exp(2\pi i/5))$. Since A_v is simple for infinitely many v, it follows that A is generically simple. Hence $\operatorname{End}^0 A = \mathbb{Q} \otimes \operatorname{End} A$ is a division algebra. By [JN, p. 178] this contains k. If $\operatorname{End}^0 A$ were any bigger, then Albert's classification (see for example [Sh, section 1]) would imply that it is a CM field of degree 8; however, the only such families are well-known to be constant, contradicting [JN, p. 179]. Hence $\operatorname{End}^0 A = k$. In fact $\operatorname{End} A$ contains the ring of integers $\mathcal{O}$ of k, and since the latter is the maximal order, we conclude that $\operatorname{End} A = \mathcal{O}$.

It follows from our theorem, for example on taking $d = 1$ and $h = \log H$ for $H \geq 3$, that the number of v in $\mathbb{Z}$ with $0 \leq v \leq H$ for which A_v is of CM type, or even $\operatorname{End} A_v \neq \mathcal{O}$, is at most $c(\log H)^\lambda$.

In our next example we define A_v for $v = (a_0, \dots, a_5)$ in $\mathbb{A}^6$ as the Jacobian of

$$y^2 = a_0 x^5 + \cdots + a_5. \tag{6.1}$$

This gives a family A over $\mathbb{Q}(\mathbb{A}^6)$. It is known that $\operatorname{End} A = \mathbb{Z}$ (see for example Theorem 6.5 of Mori's article [Mo, p. 128]). Looking at $\mathbb{Z}^6$ in $\mathbb{A}^6$, we deduce that for each $H \geq 3$ there is a non-zero polynomial P, of degree at most $c(\log H)^\lambda$, such that

$$P(a_0, \dots, a_5) = 0$$

for all rational integers $a_0, \dots, a_5$ with $0 \leq a_0, \dots, a_5 \leq H$ such that $\operatorname{End} A_v \neq \mathbb{Z}$. Now counting as in Scholium 2, p. 414, of [Ma2], we find at most $c H^5 (\log H)^\lambda$ such exceptional v, in comparison with at least H^6 altogether.

In this example the number of parameters can be cut down using the curves

$$y^2 = x(x-1)(x-\alpha)(x-\beta)(x-\gamma) \tag{6.2}$$

over $\mathbb{Q}(\mathbb{A}^3)$. It is easily seen that every curve (6.1) is isomorphic to one of these; so we conclude $\operatorname{End} A = \mathbb{Z}$ here as well. Thus there are at most $c H^2 (\log H)^\lambda$ integer triples (α, β, γ), with $0 \leq \alpha, \beta, \gamma \leq H$, for which the Jacobian of (6.2) has non-trivial endomorphism ring.

Now the triples (α, β, γ) essentially parametrize a Siegel modular 3-fold $\mathcal{S}$, and the points on the so-called Humbert surfaces correspond to abelian varieties with real multiplication (see for example [G, chap. IX]). So our theorem implies, roughly speaking, that the algebraic points on the totality of Humbert surfaces on $\mathcal{S}$ are relatively sparse.

Our final example refers to a paper [Me] of Mestre. Define A_v for $v = (u, t)$ in $\mathbb{A}^2$ as the Jacobian of

$$y^2 = (1-x)^3 + ux\big((1-x)^3 + ux^2 - x^3(1-x)\big) - tx^2(1-x)^2.$$

In [Me, p. 202] it is proved that A_v has real multiplication by the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt{5})$. On the other hand the corresponding moduli space is this time a Hilbert modular surface $\mathcal{H}$ (see [G, chap. X]). Moreover the discussion in [Me, pp. 193–194] shows that every point of $\mathcal{H}$ corresponds to some A_v. It follows that $\operatorname{End} A = \mathcal{O}$ for the associated family A over $\mathbb{Q}(\mathbb{A}^2)$. We deduce in particular that there are at most $cH(\log H)^\lambda$ integer pairs $v = (u, t)$ with $0 \le u, t \le H$ such that $\operatorname{End} A_v \neq \mathcal{O}$. Now the points on the so-called modular curves on $\mathcal{H}$ correspond to the abelian varieties with multiplication by some order in some quaternion algebra (see [G, chap. V]). So we see, again in rough terms, that the algebraic points on the totality of modular curves on $\mathcal{H}$ are relatively sparse.

BIBLIOGRAPHIE

[A] André (Y.). — *G-functions and geometry*, Aspects of Mathematics E13, Vieweg-Verlag, Braunschweig Wiesbaden, 1989.

[B] Brownawell (W.D.). — *Borne effective pour l'exposant dans le théorème des zéros*, C.R. Acad. Sci. Paris, t. **305**, 1987, p. 287–290.

[D] David (S.). — *Minorations de hauteurs sur les variétés abéliennes*, Bull. Soc. Math. France, t. **121**, 1993, p. 509–544.

[FP] Faisant (A.) and Philibert (G.). — *Quelques résultats de transcendance liés à l'invariant modulaire j*, J. Number theory, t. **25**, 1987, p. 184–200.

[G] van der Geer (G.). — *Hilbert modular surfaces.* — Springer-Verlag, Berlin Heidelberg New York London Paris Tokyo, 1988.

[H] Hartshorne (R.). — *Algebraic geometry.* — Springer-Verlag, New York Heidelberg Berlin 1977.

[JN] de Jong (J.) and Noot (R.). — Jacobians with complex multiplication, *Arithmetic algebraic geometry* (eds. G. van der Geer, F. Oort, J. Steenbrink), Progress in Math., t. **89**, Birkhäuser, Boston Basel Berlin 1991, p. 177–192.

[L] LANGE (H.). — *Equations for endomorphisms of abelian varieties*, Math. Annalen, t. **280**, 1988, p. 613–623.

[Ma1] MASSER (D.W.). — Small values of heights on families of abelian varieties, *Diophantine approximation and transcendence theory* (ed. G. Wüstholz), Lecture Notes in Math., t. **1290**, Springer-Verlag, 1987, p. 109–148.

[Ma2] MASSER (D.W.). — *Specializations of finitely generated subgroups of abelian varieties*, Trans. Amer. Math. Soc., t. **311**, 1989, p. 413–424.

[Ma3] MASSER (D.W.). — Large period matrices and a conjecture of Lang, *Séminaire de Théorie des Nombres Paris 1991–1992* (ed. S. David), Progress in Math., t. **116**, Birkhäuser, Boston Basel Berlin, 1993, p. 152–177.

[MW1] MASSER (D.W.) and WÜSTHOLZ (G.). — *Fields of large transcendence degree generated by values of elliptic functions*, Invent. Math, t. **72**, 1983, p. 407–464.

[MW2] MASSER (D.W.) and WÜSTHOLZ (G.). — *Periods and minimal abelian subvarieties*, Annals of Math., t. **137**, 1993, p. 407–458.

[MW3] MASSER (D.W.) and WÜSTHOLZ (G.). — *Endomorphism estimates for abelian varieties*, Math. Z, t. **215**, 1994, p. 641–653.

[Me] MESTRE (J.-F.). — Familles de courbes hyperelliptiques à multiplications réelles, *Arithmetic algebraic geometry* (eds. G. van der Geer, F. Oort, J. Steenbrink), Progress in Math., t. **89**, Birkhäuser, Boston Basel Berlin 1991, p. 193–208.

[Mo] MORI (S.). — *The endomorphism rings of some abelian varieties*, Japan. J. Math., t. **2**, 1976, p. 109–130.

[Na] NAKAMAYE (M.). — *Multiplicity estimates and the product theorem*, Bull. Soc. Math. France, t. **123**, 1995, p. 155–188.

[Ne] NESTERENKO (J.V.). — *Bounds for the characteristic function of a prime ideal*, Math. USSR Sbornik, t. **51**, 1985, p. 9–32 (Math. Sbornik, t. **123**, 1984, p. 11–34).

[No] NOOT (R.). — *Abelian varieties Galois representations and properties of ordinary reduction*, Compositio Math., t. **97**, 1995, p. 161–171.

[P] PHILIPPON (P.). — *Lemmes de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France, t. **114**, 1986, p. 355–383; and *Addendum*, *ibid.*, t. **115**, 1987, p. 397–398.

[Se1] SERRE (J.-P.). — *Letter to Ribet*, dated 1.1.81.

[Se2] SERRE (J.-P.). — Lectures on the Mordell-Weil theorem, *Aspects of Mathematics* E15, Vieweg-Verlag, Braunschweig Wiesbaden, 1990.

[Sh] SHIMURA (G.). — *On analytic families of polarized abelian varieties and automorphic functions*, Annals of Math., t. **78**, 1963, p. 149–192.