Endomorphism estimates for abelian varieties

D.W. Masser
and
G. Wüstholz

University of Michigan
Ann Arbor, Michigan 48109

USA

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

Germany

ETH-Zentrum
8092 Zürich

Schweiz

MPI /91-51

1. Introduction.

Let A', A'' be abelian varieties defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers. If they are isogenous, we showed in our paper [MW4] how to estimate the smallest degree of any isogeny between them. For some purposes it may be necessary to estimate all isogenies, not just a single one, and a subsidiary aim of the present article to indicate how this may be done.

In fact we will show how to find all homomorphisms from A' to A'', whether A', A'' are isogenous or not, and even if they have different dimensions. This will be achieved by the familiar device of embedding $\mathrm{Hom}(A', A'')$ into $\mathrm{End}(A' \times A'')$. Indeed our main Theorem below will enable us more generally to find all elements of the endomorphism ring $\mathrm{End}\, A$ of an arbitrary abelian variety A defined over $\overline{\mathbb{Q}}$.

We shall measure such endomorphism rings in a basis-free manner by taking suitable discriminants. But for the present paper such discriminants will depend on a choice of polarization for A. Thus let r be a positive definite element of the Néron-Severi group $NS(A)$. This gives rise to a Rosati involution on $\mathbb{Q} \otimes \mathrm{End} A$, which may be used to define the discriminant $\mathcal{D}_r(\Gamma)$ of any additive subgroup Γ of $\mathrm{End}\, A$ (for precise definitions see section 2). This turns out to be a positive rational number with denominator dividing δ^l, where δ is the degree of r and l is the rank of Γ over $\mathbb{Z}$. If A is in fact defined over a number field k, we shall take Γ as the set $\mathrm{End}_k A$ of all endomorphisms defined over k.

The following is our main result on endomorphisms, in which $h(A)$ denotes the (absolute logarithmic semistable) Faltings height of A.

Theorem *Given positive integers n, d and δ, there is a constant C, depending only on n, d and δ, and there is a constant κ, depending only on n, with the following property. Let A be an abelian variety of dimension n defined over a number field k of degree d, and let r be a positive definite element of $NS(A)$ of degree δ. Then $\mathcal{D}_r(\mathrm{End}_k A)$ is at most $C(\max\{1, h(A)\})^\kappa$.*

A similar estimate for $\mathcal{D}_r(\mathrm{End}_{\mathbb{C}} A)$ follows almost immediately. For by Lemma 3.1 of [MW3] there is a finite extension K of k, of relative degree bounded only in terms of n, such that $\mathrm{End}_{\mathbb{C}} A = \mathrm{End}_K A$; and we simply apply the above Theorem to A defined over K.

We postpone until section 6 a more detailed discussion of the consequences mentioned above for homomorphisms. For the moment we state only a Corollary about isogenies.

Our paper [MW4] quoted above in fact treats only isogenies defined over $\mathbb{C}$ (or equivalently over the algebraic closure $\overline{k}$ of k), rather than over the ground field k. While this distinction seems to be unimportant for most applications (for example the finiteness theorems proved in [MW4]), it is worth noting that our Theorem does indeed enable isogenies over k to be estimated, in the following sense.

Corollary. *Given positive integers m, d, δ' and δ'', there is a constant C, depending only on m, d, δ' and δ'', and there is a constant λ, depending only on m, with the following property. Let A', A'' be abelian varieties of dimension m defined over a number field k of degree d, with polarizations of degrees δ', δ'' respectively. Then if A', A'' are isogenous over k, there is an isogeny from A' to A'', defined over k, of degree at most $C(\max\{1, h(A')\})^\lambda$.*

Some special cases of the above Theorem and its Corollary were previously known. For an elliptic curve $(n = 1)$ the Theorem was proved some time ago by Paula Cohen (unpublished) using transcendence techniques. Surprisingly, this case is also an easy consequence (with $\kappa = 2$) of Lemme 3 (i) (p. 187) of the work of Faisant and Philibert [FP], whose proof uses nothing more than elementary class field theory. But the class field theory does not seem to extend to higher dimensions.

Also the Corollary for a pair of elliptic curves $(m = 1)$ was proved in [MW1] and [MW2], again by transcendence techniques but this time using Baker's method.

Our proofs of the Theorem and its Corollary use heavily the main result of our paper [MW3], itself also proved by Baker's method. The arguments are arranged as follows. In sections 2 and 3 we collect together a number of preliminary lemmas about Rosati forms and algebraic subgroups. In section 4 we prove a basic technical result about decompositions of endomorphisms. The deduction of the Theorem in section 5 is then a relatively easy matter, and finally in section 6 we deduce the Corollary and we make some further remarks about homomorphisms between abelian varieties.

The first author was supported in part by grants from the National Science Foundation. He would also like to thank the Forschungsinstitut für Mathematik (E.T.H. Zürich) for support on a number of occasions, as well as I.H.E.S. for hospitality and also M.R.T. (France) for support and the opportunity to deliver a series of lectures on the subject during Winter 1989.

2. The Rosati form.

Let Γ be a torsion-free finitely generated additive abelian group of rank $l \geq 1$, and let t be a real bilinear form on $\Gamma \times \Gamma$. We can then define a discriminant $\mathcal{D}(\Gamma; t)$ by

$$\mathcal{D}(\Gamma; t) = \det t(f_i, f_j)$$

for any basis elements $f_1, \ldots, f_l$ of Γ. We write $t(f) = t(f, f)$ for the associated quadratic form, and we say that t is positive semidefinite if $t(f) \geq 0$ for all f in Γ. The following simple observation provides our basic method for estimating discriminants.

Lemma 2.1 *Suppose t is positive semidefinite, and that there exists real $T \geq 0$ such that every element of Γ can be decomposed in $\mathbb{Q} \otimes \Gamma$ as a rational linear combination of elements $\tilde{f}$ of Γ with $t\left(\tilde{f}\right) \leq T$. Then $\mathcal{D}(\Gamma; t) \leq T^l$; further Γ has basis elements $f_1, \ldots, f_l$ satisfying*

$$t(f_i) \leq l^2 T \quad (1 \leq i \leq l).$$

Proof: Select basis elements of Γ, and use the hypothesis of the lemma to decompose each one into a rational linear combination of $\tilde{f}$ with $t\left(\tilde{f}\right) \leq T$. The resulting $\tilde{f}$ have rank l over $\mathbb{Z}$, so we can pick $\tilde{f}_1, \ldots, \tilde{f}_l$ from them generating a subgroup $\tilde{\Gamma}$ of Γ of finite index. Then the Hadamard inequality gives

$$\mathcal{D}(\Gamma; t) \leq \mathcal{D}\left(\tilde{\Gamma}; t\right) \leq t\left(\tilde{f}_1\right) \ldots t\left(\tilde{f}_l\right) \leq T^l.$$

Finally we produce the basis elements $f_1, \ldots, f_l$ from $\tilde{f}_1, \ldots, \tilde{f}_l$ using standard arguments, for example Lemma 8 (p. 135) of [C]. This completes the proof.

In our context, Γ is an additive subgroup of the ring $\mathrm{End} A = \mathrm{End}_{\mathbb{C}} A$ of endomorphisms of an abelian variety A of dimension n defined over $\mathbb{C}$. To specify t we fix a positive definite r in $NS(A)$ of degree δ, say. This leads to an involution on $\mathbb{Q} \otimes \mathrm{End}A$ as follows. As usual we identify r with a Riemann form on $T(A) \times T(A)$, where $T(A)$ is the tangent space of A at the origin. Now given a positive integer q, an element f in $q^{-1}\mathrm{End}A$ induces a map f_* on $T(A)$. Define f_*' as the adjoint of this with respect to r, so that

$$r\left(f_*'z, w\right) = r(z, f_*w) \tag{2.1}$$

for all z, w in $T(A)$. It will follow from the calculations below that $\delta q f_*'$ maps the period lattice $\Omega(A)$ in $T(A)$ into itself, and consequently has the form $\left(\delta q f'\right)_*$ for some f' in $(\delta q)^{-1}\mathrm{End}A$. The association of f' with f is called the Rosati involution corresponding to r.

Next, any element f of $q^{-1}\mathrm{End}A$ has a trace $\mathrm{Tr}\, f$ (see for example [Mu] p. 182). Normalizing so that the identity endomorphism has trace $2n$, we find that $\mathrm{Tr}\, f$ is in $q^{-1}\mathbb{Z}$. We define the Rosati form $t = \mathrm{t_r}$ by

$$t(f_1, f_2) = \mathrm{Tr}\left(f_1 f_2'\right) ;$$

clearly its values on $\Gamma \times \Gamma$ lie in $\delta^{-1}\mathbb{Z}$. Finally we write

$$\mathcal{D}_r(\Gamma) = \mathcal{D}(\Gamma; t_r) ,$$

which lies in $\delta^{-l}\mathbb{Z}$.

The associated quadratic form $t(f)$ is most readily computed using rational representations. Pick basis elements $\omega_1, \ldots, \omega_{2n}$ of $\Omega(A)$ and write $f_*W = MW$ for $W = (\omega_1, \ldots, \omega_{2n})^t$ and a rational matrix M (the exponent t denotes transpose). If f is in $q^{-1}\mathrm{End}A$, then qM is integral. Writing also $f_*'W = M'W$ for some real matrix M', and taking real and imaginary parts of (2.1) evaluated at the periods, we find that

$$M' = SM^tS^{-1} = EM^tE^{-1} ,$$

where S, E are the matrices with entries $\mathrm{Re}\, r(\omega_i, \omega_j)$, $\mathrm{Im}\, r(\omega_i, w_j)$ $(1 \leq i,\ j \leq 2n)$ respectively. Since E is integral with $\det E = \delta$, we see that $\delta q M'$ is integral; so, as stated above, $\delta q f_*'$ lifts to an endomorphism. We also see that

$$t(f) = \mathrm{Tr}\left(MSM^tS^{-1}\right) \tag{2.2}$$

for the usual matrix trace.

Next, S is positive definite, so we may write $S = QQ^t$ for some real Q. We then find that

$$t(f) = \mathrm{Tr}\left(XX^t\right) = \sum_{i=1}^{2n}\sum_{j=1}^{2n} (x(i,j))^2 , \tag{2.3}$$

where $X = Q^{-1}MQ$ has entries $x(i,j)$ $(1 \leq i,\ j \leq 2n)$. This makes it clear that t is positive definite. The following further properties of t will be needed in section 6.

<u>**Lemma 2.2**</u> *For* f_1, f_2 *in* End$A$ *we have* $t(f_1 f_2) \leq t(f_1)t(f_2)$.

Proof: By (2.3) it suffices to verify that

$$\mathrm{Tr}(XX^t) \leq \mathrm{Tr}(X_1X_1^t)\mathrm{Tr}(X_2X_2^t)$$

for any real X_1, X_2 with entries $x_1(i,j)$, $x_2(i,j)$ $(1 \leq i,\, j \leq 2n)$ and $X = X_1X_2$. But the left-hand side is

$$\sum_{i=1}^{2n}\sum_{j=1}^{2n}\left(\sum_{k=1}^{2n} x_1(i,k)x_2(k,j)\right)^2 = \sum_{i=1}^{2n}\sum_{j=1}^{2n}\sum_{k_1=1}^{2n}\sum_{k_2=1}^{2n} y_1y_2\,,$$

where

$$y_1 = x_1(i,k_1)x_2(k_2,j)\,, \quad y_2 = x_1(i,k_2)x_2(k_1,j)\,.$$

By the arithmetic-geometric mean inequality $y_1y_2 \leq \frac{1}{2}(y_1^2 + y_2^2)$, and summing gives $\frac{1}{2}\mathrm{Tr}(X_1X_1^t)\mathrm{Tr}(X_2X_2^t)$ twice. This proves the lemma.

Lemma 2.3 *Suppose f in* End$A$ *is an isogeny. Then it has degree at most* $(2n)^{-n}(t(f))^n$.

Proof: Since in this case f has degree $|\det M| = |\det X|$ in (2.3), it suffices to verify that

$$\det XX^t \leq (2n)^{-2n}(\mathrm{Tr}(XX^t))^{2n}$$

for any real X of order $2n$. But this is just the arithmetic-geometric mean inequality again, applied to the non-negative real eigenvalues of XX^t. The lemma is therefore proved.

3. Subgroups and endomorphisms.

Let A be an abelian variety of dimension n defined over $\mathbb{C}$, with endomorphism ring End$A$ = End$_{\mathbb{C}}A$. Choose a positive definite element r of $NS(A)$, and denote by t the associated Rosati form. Recall from section 2 of [MW3] that every algebraic subgroup B of A has a normalized degree $\Delta(B)$ with respect to r. More generally, if k is a positive integer, then r induces a natural positive definite element of $NS(A^k)$, and we may use this to define normalized degrees of algebraic subgroups of A^k.

Lemma 3.1 *Suppose for some positive integer q that H is a connected abelian subvariety of $A \times A^q$, of dimension n, which projects surjectively onto the first factor. Then there are $f_1, \ldots, f_q$ in* End$A$, *and non-zero integers $s_1, \ldots, s_q$, such that H is the maximal connected subgroup of the set of all $(a_0, a_1, \ldots, a_q)$ in $A \times A^q$ satisfying*

$$f_i(a_0) = s_ia_i \quad (1 \leq i \leq q)\,. \tag{3.1}$$

Further, we can take

$$\Delta(A)t(f_i) \leq \Delta^2(H) \quad (1 \leq i \leq q)\,. \tag{3.2}$$

Proof: We start with the case $q = 1$. Select basis elements $(\chi_1, \psi_1), \ldots, (\chi_{2n}, \psi_{2n})$ for the period lattice of H in $T(A) \times T(A)$. By Lemma 2.1 of [MW3] we have

$$\Delta^2(H) = \det(S_0 + S_1)\,, \tag{3.3}$$

where S_0, S_1 have entries $\mathrm{Re}\, r(\chi_i, \chi_j)$, $\mathrm{Re}\, r(\psi_i, \psi_j)$ $(1 \leq i, j \leq 2n)$ respectively. And if $\omega_1, \ldots, \omega_{2n}$ are basis elements of $\Omega(A)$ we can write

$$(\chi_1, \ldots, \chi_{2n})^t = M_0 W, \quad (\psi_1, \ldots, \psi_{2n})^t = M_1 W \tag{3.4}$$

for $W = (\omega_1, \ldots, \omega_{2n})^t$ and integer matrices M_0, M_1. Since H projects surjectively onto the first factor, we know that M_0 is non-singular. Also

$$S_0 = M_0 S M_0^t, \quad S_1 = M_1 S M_1^t, \tag{3.5}$$

where S has entries $\mathrm{Re}\, r(\omega_i, \omega_j)$ $(1 \leq i, j \leq 2n)$.

Now the existence of $f = f_1$, $s = s_1$ satisfying (3.1) is easy to establish using the inverse of the projection isogeny from H to A. We put $\tilde{s} = \det M_0 \neq 0$ and $\tilde{f} = s^{-1}\tilde{s}f$ in $\mathbb{Q}\otimes\mathrm{End}A$; then (3.1) holds on the tangent space with f_1, s_1 replaced by $\tilde{f}$, $\tilde{s}$. We will show that $\tilde{f}$ is actually in $\mathrm{End}A$ and satisfies (3.2); this will prove the present lemma for $q = 1$.

Since f is in $\mathrm{End}A$, we have $f_* W = MW$ for integral M, so $\tilde{f}_* W = \tilde{M} W$ for $\tilde{M} = s^{-1}\tilde{s}M$. But also $f_* \chi_i = s\psi_i$ $(1 \leq i \leq 2n)$, which leads using (3.4) to $M_0 M = sM$, so that $\tilde{M} = \tilde{s}\, M_0^{-1} M_1$. Thus $\tilde{M}$ is integral, and $\tilde{f}$ is indeed an endomorphism.

It remains to estimate $t\left(\tilde{f}\right)$. But by (2.2) and (3.5) we get

$$t\left(\tilde{f}\right) = \mathrm{Tr}\left(\tilde{M} S \tilde{M}^t S^{-1}\right) = \tilde{s}^2 \mathrm{Tr}(S_0^{-1} S_1). \tag{3.6}$$

Applying Lemma 2.1 of [MW4] to $f(x) = \det(xS_0 + S_1)$, we see that $f(1)$ is at least the coefficient of x^{2n-1}. That is,

$$\det(S_0 + S_1) \geq (\det S_0)\mathrm{Tr}(S_0^{-1} S_1),$$

and since $\det S_0 = \tilde{s}^2 \Delta(A)$ by (3.5) this gives the desired inequality (3.2) on recalling (3.3). So the present lemma is proved for $q = 1$.

The general case follows easily by labelling the factors of A^q as $A_1, \ldots, A_q$, projecting H down to each $A \times A_i$ $(1 \leq i \leq q)$, and using Lemma 2.2 of [MW4] to estimate the degrees of the images. This completes the proof.

Lemma 3.2 *Let B be a connected abelian subvariety of A, and for a positive integer q let H be an algebraic subgroup of $A \times B^q$ in $A \times A^q$ which projects surjectively onto the first factor. Then either*

(α) there is a positive integer $\tilde{q} \leq q$ and a subproduct $B^{\tilde{q}}$ of B^q such that the intersection $\tilde{H}$ of H with $A \times B^{\tilde{q}}$ also projects surjectively onto the first factor; further $\tilde{H}$ has dimension n and $\Delta\left(\tilde{H}\right) \leq \Delta(H)$, or

(β) there is a connected abelian subvariety B' of B with $0 \neq B' \neq B$ and $\Delta(B') \leq \Delta(H)$.

Proof: We use induction on q. The case $q = 1$ is trivial, since (α) always holds with $\tilde{q} = 1$. Suppose the result has been proved with q replaced by $q - 1$ for some $q \geq 2$. We will deduce the lemma as it stands.

For this we look at the algebraic subgroup K of B^q such that $0 \times K$ is the maximal connected subgroup of the intersection of H with $0 \times A^q$. In the terminology of section 2 of [MW4], K is the maximal connected subgroup of the kernel of H in A^q. If $K = 0$ then (α) holds with $\tilde{q} = q$, since the projection from H to A is an isogeny.

So we can assume $K \neq 0$. Rearranging the factors of B^q if necessary, we can also assume $B' \neq 0$, where B' is the projection of K to the last factor. If $B' \neq B$ then (β) holds. For then two applications of Lemma 2.2 of [MW4] show that

$$\Delta(B') \leq \Delta(K) \leq \Delta(H)$$

as required.

So we can assume $B' = B$. In that case define H_1 in $A \times B^{q-1}$ such that $H_1 \times 0$ is the intersection of H with $A \times A^{q-1} \times 0$. We will verify that the induction hypothesis applies to H_1. To see that H_1 projects surjectively onto A, take arbitrary a in A. Since H projects surjectively, there exists β in B^{q-1} and b in B such that (a, β, b) is in H. But also there exists β' in B^{q-1} such that (β', b) is in K; so $(0, \beta', b)$ is in H. Subtracting, we find that $(a, \beta - \beta', 0)$ is in H, and thus $(a, \beta - \beta')$ is in H_1. Since a was arbitrary, this does what we want.

We can therefore apply our induction hypothesis to H_1. Since $\Delta(H_1) \leq \Delta(H)$ again by Lemma 2.2 of [MW4], each of the conditions (α) and (β) for H_1 evidently implies the same condition for H. This completes the proof of the present lemma.

4. The decomposition

In this section we prove the main technical result on decompositions which, combined with Lemma 2.1, enables us to prove the Theorem. We shall make essential use of the main result of [MW3] (see especially section 11), which we therefore state here as follows. Let G be a principally polarized abelian variety of dimension g defined over a number field of degree d, and let r be a positive definite element of $NS(G)$ of degree 1. Then for any period ω in $\Omega(G)$ the minimal abelian subvariety G_ω whose tangent space contains ω satisfies

$$\Delta(G_\omega) \leq c(\max\{d, h(G), r(\omega)\})^{\kappa_0}. \qquad (4.1)$$

Here κ_0 and c depend only on g; and in fact we can take $\kappa_0 = (g-1).4^g g!$

Throughout this section A will be an abelian variety of dimension n, and End$A$ will as usual denote its ring of endomorphisms over $\mathbb{C}$. Let K be the maximum of the exponents $\kappa_0(g)$ in (4.1) for all positive integers $g \leq n(2n+1)$. We define non-negative integers $\delta(0)$, $\delta(1)$, ... by

$$\delta(0) = 0,\ \delta(m) = 2n(2n-1)K + (2nK+1)\delta(m-1) \qquad (m \geq 1),$$

and we define similarly

$$\tau(0) = 0,\ \tau(m) = 4n(2n-1)K + 4nK\delta(m-1) \qquad (m \geq 1).$$

These numbers of course depend on n as well as m.

Proposition *Given integers m, n with $n \geq 1$ and $0 \leq m \leq n$, there is a constant $c = c(m, n)$ with the following property. Let A be a principally polarized abelian variety of dimension n*

defined over a number field of degree d, *and let* r *be a positive definite element of* $NS(A)$ *of degree 1. Then every element of* End$A$ *can be decomposed in* $\mathbb{Q} \otimes \mathrm{End}A$ *as a rational linear combination of elements* f *in* End$A$ *such that either*

(α_m) $\quad t(f) \leq cM^{\tau(m)}$

or

(β_m) $f(A)$ *is contained in an abelian subvariety* $B = B(f)$ *in* A, *of dimension at most* $n-m$, *with* $\Delta(B) \leq cM^{\delta(m)}$. *Here*

$$M = \max\{d, h(A)\}\,.$$

Proof: This is by induction on m. The case $m = 0$ is trivial, since we can take a single element of the class (β_0) with $B = A$.

Assume therefore that we have proved the Proposition with m replaced by $m-1$ for some m with $1 \leq m < n$. We proceed to deduce the Proposition as it stands. Now any f in the class (α_{m-1}) is already in the class (α_m). We will show that any f in the class (β_{m-1}) either splits into elements of the class (α_m) or splits into elements of the class (β_m), for suitably adjusted constants c. This will establish the Proposition.

We use c_1, c_2, ... for positive constants depending only on m and n. Let f be any endomorphism of class (β_{m-1}) ; thus $f(A)$ is contained in an abelian subvariety B in A of dimension $p \leq n-m+1$ with

$$\Delta = \Delta(B) \leq c_1 M^{\delta(m-1)}\,. \tag{4.2}$$

We proceed to decompose f.

By Lemma 4.2 of [MW4] there are basis elements $\chi_1, \ldots, \chi_{2p}$ of the period lattice $\Omega(B)$ of B such that

$$r(\chi_j) \leq c_2 M^{2(2p-1)}\Delta^2 \quad (1 \leq j \leq 2p)\,. \tag{4.3}$$

Similarly there are basis elements $\omega_1, \ldots \omega_{2n}$ of $\Omega(A)$ such that

$$r(\omega_i) \leq c_3 M^{2(2n-1)} \quad (1 \leq i \leq 2n)\,, \tag{4.4}$$

since $\Delta(A) = 1$. We may arrange these so that $\omega_1, \ldots, \omega_n$ are linearly independent over $\mathbb{C}$.

Since f maps A into B , we have equations on the tangent space

$$f_* \omega_i = \sum_{j=1}^{2p} s_{ij} \chi_j \quad (1 \leq i \leq 2n) \tag{4.5}$$

for integers s_{ij} $(1 \leq i \leq 2n,\ 1 \leq j \leq 2p)$. We apply (4.1) to $G = A \times A^{2p}$ with the period $(\omega_i, \chi_1, \ldots, \chi_{2p})$ for each i with $1 \leq i \leq n$. We obtain minimal algebraic subgroups H_i of G with tangent spaces containing $(\omega_i, \chi_1, \ldots, \chi_{2p})$. Also H_i lies inside the algebraic subgroup Γ_i of G defined as the set of $(a_0, a_1, \ldots a_{2p})$ in $A \times B^{2p}$ satisfying

$$f(a_0) = \sum_{j=1}^{2p} s_{ij} a_j\,. \tag{4.6}$$

Noting that $h(G) = (2p+1)h(A)$, we get using (4.3) and (4.4)

$$\Delta(H_i) \leq c_4 M^{2(2n-1)K} \Delta^{2K} \quad (1 \leq i \leq n)\,. \tag{4.7}$$

Let ϵ_i be the embedding of $A \times A^{2p}$ inside $A \times A^{2pn}$ defined by

$$\epsilon_i(a, \alpha) = (a, 0, \ldots, 0, \alpha, 0, \ldots, 0)$$

for a in A, α in A^p, where the α is in the $i-$th place out of n places $(1 \leq i \leq n)$. We define $H = \sum_{i=1}^{n} \epsilon_i(H_i)$ as a subgroup of $A \times B^{2pn}$ in $A \times A^{2pn}$. By Lemma 2.2 of [MW3] and (4.7) above we have

$$\Delta(H) \leq \prod_{i=1}^{n} \Delta(\epsilon_i(H_i)) = \prod_{i=1}^{n} \Delta(H_i) \leq c_5 M^{2n(2n-1)K} \Delta^{2nK}\,. \tag{4.8}$$

Now the tangent space of the projection of H to the first factor contains $\omega_1, \ldots, \omega_n$; so by our choice of these periods this tangent space must be all of $T(A)$. In other words, H projects surjectively onto the first factor. We may therefore apply Lemma 3.2, and we consider each of the alternative conclusions (α), (β) in turn.

Suppose first (β) holds, so that B has a connected abelian subvariety B' with $0 \neq B' \neq B$ and

$$\Delta(B') \leq \Delta(H)\,. \tag{4.9}$$

Let B'' be the abelian variety orthogonal to B' in B. Then

$$\Delta(B'') \leq \Delta(B)\Delta(B') \leq \Delta(B)\Delta(H) \tag{4.10}$$

by Lemma 2.3 in [MW3]. Since $B' + B'' = B$ the map f from A to B may now be written as a rational linear combination of maps f' from A to B' and f'' from A to B''. Both B' and B'' have dimensions at most $p - 1 \leq n - m$, and their normalized degrees are at most

$$\Delta(B)\Delta(H) \leq c_5 M^{2n(2n-1)K} \Delta^{2nK+1} \leq c_6 M^{\delta(m)}$$

by (4.2), (4.8), (4.9), (4.10) and the definition of $\delta(m)$.

Thus we find that in case (β) of Lemma 3.2 the f in class (β_{m-1}) of the Proposition decomposes into (two) endomorphisms of the class (β_m).

Now we consider case (α) of Lemma 3.2. We denote the variables of $\epsilon_i(0 \times A^{2p})$ in $0 \times A^{2pn}$ by $(a_{i1}, \ldots, a_{i,2p})$, so that the factors of A^{2pn} are indexed by the set Q of pairs (i,j) with $1 \leq i \leq n$, $1 \leq j \leq 2p$. Now the subproduct in Lemma 3.2 corresponds to a non-empty subset $\tilde{Q}$ of Q, and we get $\tilde{H}$ with $\Delta\left(\tilde{H}\right) \leq \Delta(H)$. We can apply Lemma 3.1 to $\tilde{H}$, or rather its maximal connected subgroup $\tilde{H}^0$. We find for each (i,j) in $\tilde{Q}$ an endomorphism $\tilde{f}_{ij}$ and a non-zero integer $\tilde{s}_{ij}$ such that $\tilde{H}^0$ is the maximal connected subgroup of the set defined by

$$\tilde{f}_{ij}(a_0) = \tilde{s}_{ij} a_{ij}\,. \tag{4.11}$$

Further, we can take

$$t\left(\tilde{f}_{ij}\right) \leq \Delta^2\left(\tilde{H}\right) \leq \Delta^2(H) \leq c_7 M^{\tau(m)} \tag{4.12}$$

by (4.2), (4.8) and the definition of $\tau(m)$.

On the other hand recall that each H_i is contained in the subgroup Γ_i of $A \times A^{2p}$. So $H = \sum_{i=1}^{n} \epsilon_i(H_i)$ is contained in $\Gamma = \sum_{i=1}^{n} \epsilon_i(\Gamma_i)$. From (4.6) we see that Γ is defined in $A \times B^{2pn}$ by $f(a_0) = \sum s_{ij}a_{ij}$ where the sum is over Q. Therefore $\tilde{H}$, and so also $\tilde{H}^0$, are contained in the set $\tilde{\Gamma}$ defined by

$$f(a_0) = \tilde{\sum} s_{ij}a_{ij}\,, \tag{4.13}$$

where now the sum is over all (i,j) in $\tilde{Q}$.

Finally substituting (4.11) into (4.13) we obtain f as a rational linear combination of the $\tilde{f}_{ij}$ satisfying (4.12). Thus we find that in case (α) of Lemma 3.2 the f in class (β_{m-1}) of the Proposition decomposes into endomorphisms of the class (α_m).

As noted above, this suffices to prove the Proposition by induction on m.

5. Proof of Theorem

Let A and r be as in the Theorem. Again the positive constants $c_1, c_2, \ldots$ will depend only on n. By Lemma 5.3 of [MW3], there is a principally polarized abelian variety A_1, a positive definite r_1 in $NS(A_1)$ of degree 1, and an isogeny g from A to A_1 of degree $\sqrt{\delta}$ with $g_* r_1 = r$. Further A_1 is defined over a number field of degree $d_1 \leq c_1 d\delta^n$. From the decomposition of $\mathrm{End}A_1 = \mathrm{End}_{\mathbb{C}}A_1$ over $\mathbb{C}$ in the Proposition for $m = n$, we shall deduce an analogous decomposition of $\mathrm{End}_k A$ over k.

We use the group homomorphism λ_1 from $\mathrm{End}_{\mathbb{C}}A$ to $\mathrm{End}_{\mathbb{C}}A_1$ given by $\lambda_1(f) = gf\hat{g}$, where $\hat{g}$ denotes the isogeny from A_1 to A such that $g\hat{g}$, $\hat{g}g$ are multiplication by $\sqrt{\delta}$. We also have a map λ in the opposite direction given by $\lambda(f_1) = \hat{g}f_1 g$.

Pick any f in $\mathrm{End}_k A$. Then $f_1 = \lambda_1(f)$ is in $\mathrm{End}_{\mathbb{C}}A_1$, so by the Proposition with $m = n$ it can be written as a rational linear combination of elements $\tilde{f}_1$ of $\mathrm{End}_{\mathbb{C}}A_1$ with

$$t_1\left(\tilde{f}_1\right) \leq c_2(\max\{d_1, h(A_1)\})^{\tau}\,,$$

where $\tau = \tau(n)$ and t_1 corresponds to r_1. Applying λ, we see that $\lambda(f_1) = \delta f$ can be written as a rational linear combination of elements $\tilde{f}' = \lambda\left(\tilde{f}_1\right)$ of $\mathrm{End}_{\mathbb{C}}A$. Also it is not difficult using (2.1) to check that $t\left(\tilde{f}'\right) = \delta t_1\left(\tilde{f}_1\right)$. Thus f itself has a rational decomposition into elements $\tilde{f}'$ of $\mathrm{End}_{\mathbb{C}}A$ with

$$t\left(\tilde{f}'\right) \leq c_2\delta(\max\{d_1, h(A_1)\})^{\tau}\,.$$

Now $d_1 \leq c_1 d\delta^n$ and we have

$$h(A_1) \leq h(A) + \frac{1}{4}\log\delta$$

by equation (8.2) of [MW3]. So we end up with

$$t\left(\tilde{f}'\right) \leq c_3\delta(\max\{d\delta^n, h(A)\})^\tau . \tag{5.1}$$

But even though f is in $\mathrm{End}_k A$, the $\tilde{f}'$ are not necessarily in $\mathrm{End}_k A$. To get around this we take conjugates. By Lemma 3.1 of [MW3] all elements of $\mathrm{End}_{\mathbb{C}} A$ are in fact defined over some extension k_0 of k of relative degree $e \leq c_4$. For each complex embedding σ of k_0 fixing k, apply σ to the above decomposition of f, and average over σ. We obtain a new decomposition of f into elements $\tilde{f}$ of $\mathrm{End}_{\mathbb{C}} A$, each of which is the sum of e conjugates of a fixed $\tilde{f}'$, and therefore in $\mathrm{End}_k A$. Since t is Galois-invariant, the Cauchy-Schwarz inequality gives

$$t\left(\tilde{f}\right) \leq e^2 t\left(\tilde{f}'\right) . \tag{5.2}$$

We may now apply Lemma 2.1 to $\mathrm{End}_k A$, and (5.1), (5.2) yield

$$\mathcal{D}_\tau(\mathrm{End}_k A) \leq c_5\delta^l(\max\{d\delta^n, h(A)\})^{l\tau} , \tag{5.3}$$

where l is the rank of $\mathrm{End}_k A$. This implies the Theorem, with exponent

$$\kappa = l\tau$$

and

$$C \leq c_5\delta^l(d\delta^n)^\kappa .$$

As for the exponent, one verifies easily that $\tau(n) = 4n(2n-1)K(2nK+1)^{n-1}$. Since $l \leq 4n^2$, we have

$$\kappa \leq 16n^3(2n-1)K(2nK+1)^{n-1} .$$

By section 4 we can also take

$$K = (N-1)4^N N!, \quad N = n(2n+1) ,$$

and so the upper bound for κ is enormous, of order n^{4n^3} for n large.

Perhaps one might expect the Theorem to hold with $\kappa = 0$, but this probably lies much deeper; for example, the result for $n = 1$ and $\kappa < 2$ would already imply the Baker-Stark Theorem. For if $\mathcal{O}$ is the ring of integers of a complex quadratic field k of discriminant $-D < 0$ and class number 1, the elliptic curve $E = \mathbb{C}/\mathcal{O}$ is defined over $\mathbb{Q}$ and $\mathcal{D}_\tau(\mathrm{End}_k E) = D$ for the unique principal polarization; whereas $h(E)$ has order at most $\sqrt{D}$ by the Fourier expansion of the elliptic modular function. Also, as already pointed out in section 6 of [MW4], the crucial estimate (4.1) is false for $\kappa_0 = 0$, so there seems very little chance of obtaining $\kappa = 0$ by the present methods.

In preparation for the next section, we record the following additional consequence of our arguments.

Lemma 5.1 *The additive group* $\mathrm{End}_k A$ *has basis elements* $f_1, \ldots, f_l$ *satisfying*

$$t(f_i) \leq c_6\delta(\max\{d\delta^n, h(A)\})^\tau \quad (1 \leq i \leq l) .$$

Proof: We simply apply the other part of Lemma 2.1 to find these basis elements, again using the inequalities (5.1), (5.2).

6. Proof of Corollary

Let A', A'' be abelian varieties, possibly of different dimensions, defined over a number field k. We start by indicating a general method of finding all elements of $\mathrm{Hom}_k(A', A'')$, and we then carry out the estimates needed to establish the Corollary for isogenies.

Write $A = A' \times A''$; then the elements f of $\mathrm{End}_k A$ may be represented as matrices $\begin{pmatrix} f' & g'' \\ g' & f'' \end{pmatrix}$ for f' in $\mathrm{End}_k A'$, g'' in $\mathrm{Hom}_k(A', A'')$, g' in $\mathrm{Hom}_k(A'', A')$, and f'' in $\mathrm{End}_k A''$. If we have polarizations of degrees δ', δ'' on A', A'' respectively, then we have a natural polarization of degree $\delta = \delta'\delta''$ on A, and we can accordingly use Lemma 5.1 to find basis elements $f_1, \ldots, f_l$ of $\mathrm{End}_k A$. Clearly the corresponding $g_1'', \ldots, g_l''$ generate $\mathrm{Hom}_k(A', A'')$.

So in this sense we can find all elements of $\mathrm{Hom}_k(A', A'')$, but it is difficult to be more precise until we provide a suitable way of measuring such elements. One general way, though not very canonical, is to use rational representations as in section 2. For isogenies, however, there is no problem, and we proceed to illustrate this by proving the Corollary.

Now A has dimension $n = 2m$, and Lemma 5.1 gives

$$t(f_i) \leq T = c_1 \delta (\max\{d\delta^n, h(A)\})^\tau \quad (1 \leq i \leq l) . \tag{6.1}$$

Here d is the degree of k, and t is the Rosati form corresponding to the product polarization on A. For this section $c_1, c_2, \ldots$ will denote positive constants depending only on m.

To recover estimates for the g'' we use the matrix identity

$$\begin{pmatrix} 1' & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} f' & g'' \\ g' & f'' \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1'' \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1'' \end{pmatrix}\begin{pmatrix} f' & g'' \\ g' & f'' \end{pmatrix}\begin{pmatrix} 1' & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & g'' \\ g' & 0 \end{pmatrix} \tag{6.2}$$

where $1'$, $1''$ are the identity endomorphisms of A', A'' respectively. With the obvious abbreviations ι', ι'' , we define a corresponding group homomorphism μ from $\mathrm{End}_k A$ to $\mathrm{End}_k A$ by

$$\mu(f) = \iota' f \iota'' + \iota'' f \iota' .$$

It is well-known (see for example [Mu] p. 174) that the degree function is a homogeneous polynomial of degree $2n$ on $\mathrm{End}_k A$. In particular there exists a polynomial $P = P(x_1, \ldots, x_l)$, homogeneous of degree $2n$, such that whenever $m_1, \ldots, m_l$ are integers, the value $P(m_1, \ldots, m_l)$ is the degree of the endomorphism

$$\tilde{f} = m_1\mu(f_1) + \ldots + m_l\mu(f_l) = \mu(m_1 f_1 + \ldots + m_l f_l)$$

(interpreted as 0 if $\tilde{f}$ is not an isogeny).

We claim that P is not identically zero. For by hypothesis there exists an isogeny $\tilde{g}''$ from A' to A'' over k , and so there also exists an isogeny $\tilde{g}'$ from A'' to A' over k. Putting $f' = 0 = f''$ in (6.2), we see that $\tilde{f} = \begin{pmatrix} 0 & \tilde{g}'' \\ \tilde{g}' & 0 \end{pmatrix}$ satisfies $\tilde{f} = \mu\left(\tilde{f}\right)$; and since $\tilde{f}$ is also an isogeny we see that P takes a non-zero value. So indeed P is not identically zero.

A standard argument using the Lagrange Interpolation Formula now shows that we can find integers $m_1, \ldots, m_l$ with

$$0 \leq m_1, \ldots, m_l \leq 2n \tag{6.3}$$

such that $p = P(m_1, \dots, m_l) \neq 0$. Thus for $f = m_1 f_1 + \dots + m_l f_l$ we see that $\mu(f)$ is an isogeny of degree p. It follows that $\mu(f) = \begin{pmatrix} 0 & g'' \\ g' & 0 \end{pmatrix}$ for isogenies g'', g' both of degrees at most p. From Lemma 2.3 we have $p \leq (2n)^{-n}(t(\mu(f)))^n$. Also $t(\iota') = t(\iota'') = 2m$ using (2.2), and Lemma 2.2 shows that $t(\iota' f \iota'')$, $t(\iota'' f \iota')$ are both at most $4m^2 t(f)$. So by Cauchy-Schwarz we get $t(\mu(f)) \leq 16m^2 t(f)$. A second application of Cauchy-Schwarz using (6.1) and (6.3) gives $t(f) \leq 4n^2 l^2 T$, and combining all these we end up with

$$p \leq c_2 \delta^n (\max\{d\delta^n, h(A)\})^{n\tau} . \tag{6.4}$$

However, $h(A) = h(A') + h(A'')$, and so (6.4) depends on the forbidden term $h(A'')$. We eliminate this exactly as in section 6 of [MW4]. Let p_0 be the smallest degree of any isogeny over k from A' to A''. By (8.2) of [MW3] we have

$$h(A'') \leq h(A') + \frac{1}{2}\log p_0 .$$

Also $p_0 \leq p$, so (6.4) now gives

$$p_0 \leq c_2 \delta^n \left(\max \left\{ d\delta^n, 2h(A') + \frac{1}{2}\log p_0 \right\} \right)^{n\tau} .$$

From this we obtain the estimate of the Corollary, with the exponent

$$\lambda = n\tau$$

and

$$C \leq c_3 \delta^n (d\delta^n)^\lambda .$$

This completes the proof.

Finally, we note that in the situation of the Corollary, a set of generators of $\mathrm{Hom}_k(A', A'')$ can be found, at least up to finite index, simply by composing the isogeny just constructed with basis elements of $\mathrm{End}_k A'$ chosen according to Lemma 5.1. This provides an alternative to the procedure outlined at the beginning of the present section.

References

[C] J.W.S. Cassels, An introduction to the geometry of numbers, Springer, Berlin-Göttingen-Heidelberg 1959.

[FP] A. Faisant and G. Philibert, Quelques résultats de transcendence liés à l'invariant modulaire j.

J. Number Theory 25 (1987), 184–200.

[MW1] D.W. Masser and G. Wüstholz, Estimating isogenies on elliptic curves, Inventiones Math. 100 (1990), 1–24.

[MW2] D.W. Masser and G. Wüstholz, Some effective estimates for elliptic curves, Arithmetic of complex manifolds (eds W.-P. Barth and H. Lange), Lecture Notes in Math. Vol. 1399, Springer 1989 (pp 103–109).

[MW3] D.W. Masser and G. Wüstholz, Periods and minimal abelian subvarieties, ETH Preprint, February 1991.

[MW4] D.W. Masser and G. Wüstholz, Isogeny estimates for abelian varieties, and finiteness theorems, preprint 1991.

[Mu] D. Mumford, Abelian varieties, Oxford 1970.