Isogeny estimates for abelian varieties, and finiteness theorems

D.W. Masser (1)
G. Wüstholz (2)

(1)
University of Michigan
Ann Arbor

(2)
ETH Zürich

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

Germany

MPI/91-28

1. Introduction.

In our paper [MW1] we showed how to estimate isogenies between elliptic curves defined over number fields. In the subsequent note [MW2] we made several arithmetic applications, notably some effective versions of the finiteness of the number of isomorphism classes of such elliptic curves within a single isogeny class.

In the present paper we generalize our isogeny estimates to abelian varieties of arbitrary dimension. We also prove the corresponding finiteness theorem, referred to by Lang [L] as Finiteness I; namely, if A is an abelian variety defined over a number field k, there are only finitely many $k-$ isomorphism classes of abelian varieties A^* defined over k that are $k-$ isogenous to A. This latter result is not new; it is an immediate consequence of the Shafarevich Conjecture for abelian varieties which was first established by Faltings in his pioneering paper [F]. Conversely, it is by now well-known that Finiteness I implies, in a relatively simple manner, not only the Shafarevich Conjecture but also all the other main results of [F]; in particular the Tate Conjecture for abelian varieties (after Tate himself) and the Mordell Conjecture for curves (after Parshin). See for example Chapter VIII of the Szpiro seminar [Sz] or the encyclopaedia article [L] of Lang.

Our work may therefore be viewed as providing new proofs of these results. But our approach through isogeny estimates often leads to additional information, usually in the form of strong upper bounds. To illustrate this we prove in the present paper a quantitative version of Finiteness I, which gives estimates involving the height of A^*. Raynaud in [Sz] has also obtained estimates for the same quantities. It is not straightforward to compare our work with his, but it appears that neither set of estimates includes the other. In a later paper we will consider the more difficult problem of estimating the isomorphism classes themselves of A^*. Also in another paper we will apply our isogeny estimates directly to obtain quantitative versions of Serre's well-known theorem [Se] on Galois groups of division fields of elliptic curves.

Our proof of Finiteness I is rather different from Faltings's proof, and it is interesting to compare the two approaches. In [F] Faltings first defines a new notion of the height of an abelian variety, and he proves a fundamental finiteness result for this height. He then uses Tate's theory of p-divisible group schemes and a theorem of Raynaud on p-power group schemes to establish the appropriate invariance of height under isogeny. The combination yields Finiteness I. It is these latter arguments on group schemes that were extended by Raynaud in [Sz] to give his effective version of Finiteness I mentioned above .

In the present paper we deduce Finiteness I rather quickly from our isogeny estimates. These in turn are deduced in an elementary way from our earlier work [MW3] on periods and minimal abelian subvarieties. This latter work belongs to the area of diophantine approximation; indeed the underlying technique is Baker's method in the theory of transcendental numbers. Actually at one point in [MW3] we make use of a quantitative version of Faltings's finiteness result for heights, so the two approaches are not completely disjoint.

In order to state our isogeny estimates let $h(A)$ denote the (absolute logarithmic semistable) Faltings height of an abelian variety A defined over a number field k. We emphasize that, throughout this paper, all isogenies and polarizations are not assumed to be defined over k unless otherwise stated; further the isogenies are not assumed to respect the polarizations.

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, A^* be abelian varieties of dimensions at most n, defined over a number field of degree at most d, with polarizations of degree at most δ. Then, if A, A^* are isogenous, there is an isogeny from A to A^* of degree at most $C(\max\{1, h(A)\})^\kappa$.*

In fact we find the values

$$\kappa = 14n^2\left(4N.4^N N!\right)^n \qquad N = n(2n+1)$$

and

$$C = cd^\kappa \delta^{(2\kappa+1)n}$$

for c depending only on n.

The arrangement of this paper is as follows. In section 2 we prove an inequality for degrees of abelian varieties that supplements those of sections 2 of [MW3]. We apply these inequalities in section 3 to obtain an extension of the Isogeny Lemma of [MW1] to abelian varieties. In section 4 we record an estimate for periods, and then in section 5 we combine this with the fundamental work of [MW3] to establish two preliminary estimates for isogenies. Our theorem is now deduced rather easily in section 6. Finally in section 7 we prove our quantitative version of Finiteness I.

The first author was supported in part by grants from the National Science Foundation. He would also like to thank the Forschungsinstitut für Mathematik (ETH 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. In addition both authors want to thank the Institute for Advanced Study (Princeton) for further support and hospitality.

2. Degrees

We prove here a new inequality for degrees of algebraic subgroups of an abelian variety. To establish the underlying matrix inequality we need first the following observation.

Lemma 2.1. *Suppose S_0, S_1 are real symmetric positive semidefinite matrices of the same order. Then all coefficients of the polynomial $\det(xS_0 + S_1)$ are non-negative.*

Proof: Assume first that S_0, S_1 are positive definite. It is well-known that they are then simultaneously diagonalizable, and for diagonal matrices the result is clear. The general case follows by continuity.

In this lemma we choose

$$S_0 = \begin{pmatrix} P_0 & Q_0 \\ Q_0^t & R_0 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 0 & 0 \\ 0 & R_1 \end{pmatrix}$$

with R_0, R_1 of the same order, and Q_0^t the transpose of Q_0. We find that

$$\det(S_0 + S_1) \geq (\det\ R_1)(\det\ P_0), \tag{2.1}$$

for it is easily checked that the right-hand side of (2.1) is the coefficient of x^m in $f(x) = \det(xS_0 + S_1)$, where m is the order of P_0, while the left-hand side is of course $f(1)$.

Now let A_1, A_2 be abelian varieties, and suppose B is an algebraic subgroup of the product $A_1 \times A_2$. We have projections π_1, π_2 from $A_1 \times A_2$ to A_1, A_2 respectively, and we call $B_1 = \pi_1(B)$ the image of B in A_1. Also π_1 restricted to B has a kernel K, and we call $C_2 = \pi_2(K)$ the kernel of B in A_2.

Fix positive definite elements of the Néron-Severi groups of A_1, A_2. For any non-negative integers m_1, m_2 we can form in a natural way a positive definite element of the Néron-Severi group of $A = A_1^{m_1} \times A_2^{m_2}$. If now B is an algebraic subgroup of A, we can define as in section 2 of [MW3] the connectivity $\kappa(B)$, the period lattice $\Omega(B)$, and the normalized degree $\Delta(B)$.

Lemma 2.2. *Suppose B is an algebraic subgroup of $A_1 \times A_2$. Let B_1 be the image of B in A_1 and let C_2 be the kernel of B in A_2. Then*

$$\Delta(B_1)\Delta(C_2) \leq \Delta(B)$$

Proof: For a subgroup X of the period lattice $\Omega(A)$ of $A = A_1 \times A_2$ we write $\delta(X)$, as in section 2 of [MW3], for the positive square root of the determinant of the real part of the associated Riemann form. If O_1 is the origin of A_1, then $Y_2 = \Omega(O_1 \times C_2)$ is a primitive subgroup of $X = \Omega(B)$. We can therefore compute $\delta(X)$ by choosing a basis for Y_2 and extending it to a basis of X. Using (2.1), we find that

$$\delta(X) \geq \delta(X_1)\delta(Y_2), \tag{2.2}$$

where X_1 is the projection of X to the tangent space of A_1. In addition we have

$$\kappa(B)\delta(X) = \Delta(B), \quad \kappa(C_2)\delta(Y_2) = \Delta(C_2). \tag{2.3}$$

There is also an obvious exact sequence

$$0 \to C_2 \to B \to B_1 \to 0,$$

and taking connected parts yields the exact sequence

$$0 \to C_2' \to B^0 \to B_1^0 \to 0, \tag{2.4}$$

where B^0, B_1^0 are the maximal connected subgroups of B, B_1 respectively, and C_2' is the kernel of B^0 in A_2. The quotient now gives

$$\kappa(B)\kappa(C_2') = \kappa(B_1)\kappa(C_2). \tag{2.5}$$

Finally the Snake Lemma applied to (2.4) as in the proof of Lemma 2.2 of [MW3] shows that X_1 has index $\kappa(C_2')$ in $\Omega_1 = \Omega(B_1)$, and so

$$\kappa(C_2')\Delta(B_1) = \kappa(C_2')\kappa(B_1)\delta(\Omega_1) = \kappa(B_1)\delta(X_1). \tag{2.6}$$

Now the inequality of the present lemma follows on combining (2.2), (2.3), (2.5) and (2.6). This completes the proof.

3. Isogenies.

The main result of this section generalizes the Isogeny Lemma (p. 5) of [MW1] from elliptic curves to abelian varieties. If A_1, A_2 are abelian varieties, we say that an algebraic subgroup B of $A_1 \times A_2$ is split (with respect to A_1, A_2) if it has the form $B_1 \times B_2$ for algebraic subgroups B_1 of A_1, B_2 of A_2. Otherwise we say that B is non-split. We require the following preliminary observation.

Lemma 3.1. *Let A, A', A'' be abelian varieties, and let B be a connected abelian subvariety of $A \times A' \times A''$. Let B' be the image of B in $A \times A'$, and let B'' be the maximal connected subgroup of the kernel of B in $A \times A''$. Then if B is non-split with respect to A, $A' \times A''$, either*

(i) B' is non-split with respect to A, A',

or

(ii) B'' is non-split with respect to A, A''.

Proof: Suppose to the contrary that B is non-split with respect to A, $A' \times A''$ but that (i) and (ii) are both false. Let O', O'' be the origins of A', A'' respectively, and denote by π the projection from $A \times A' \times A''$ to A. Pick arbitrary a in $\pi(B')$; then, since B' is split, (a, O') is in B'. So there is a'' in A'' such that (a, O', a'') is in B. Thus $m(a, a'')$ is in B'' for some positive integer m, and hence ma is in $\pi(B'')$. Since a was arbitrary and $\pi(B')$ is connected, we conclude that $\pi(B')$ is contained in $\pi(B'')$.

Once again take arbitrary a in $\pi(B) = \pi(B')$; now since B'' is split we deduce that (a, O'') is in B''. Hence (a, O', O'') is in B. Since a was arbitrary, it follows easily that B is split with respect to A, $A' \times A''$. This contradiction proves the present lemma.

For the next result, the generalized Isogeny Lemma, we carry over from section 2 the conventions about degrees of algebraic subgroups of products $A_1^{m_1} \times A_2^{m_2}$. Suppose A_1, A_2 have dimensions at most n.

Lemma 3.2. *For positive integers m_1, m_2 let B be a connected abelian subvariety of $A_1^{m_1} \times A_2^{m_2}$. Then if B is non-split with respect to $A_1^{m_1}$, $A_2^{m_2}$, there exist connected abelian subvarieties A_1', A_2' of A_1, A_2 respectively, of positive dimensions, with*

$$M = \max\{\Delta(A_1'), \Delta(A_2')\} \leq \Delta^2,$$

and an isogeny from A_1' to A_2' of degree at most $(M\Delta)^{2n}$, where $\Delta = \Delta(B)$.

Proof: We start with the case $m_1 = m_2 = 1$. Let B_1, B_2 be the images of B in A_1, A_2, and let C_1, C_2 be the kernels of B in A_1, A_2. From the well-known "Goursat's Lemma" in group theory we obtain an isomorphism f between B_1/C_1 and B_2/C_2. Also these are abelian varieties of dimension m, say, and f is an isomorphism of abelian varieties. Further, the assumption that B is non-split means that $m > 0$. Let C_1^0, C_2^0 be the maximal connected subgroups of C_1, C_2, and define A_1', A_2' as the orthogonal complements of C_1^0, C_2^0 in B_1, B_2 respectively.

Now there is an obvious homomorphism from A_1' to B_1/C_1, and this is an isogeny of degree $D_1 = \Delta(A_1' \cap C_1)$. By Lemma 2.2 of [MW3] we have

$$D_1 \leq \Delta(A_1')\Delta(C_1). \tag{3.1}$$

From Lemma 2.3 of [MW3] we see that

$$\Delta(A_1') \leq \Delta(B_1)\Delta(C_1^0)\,, \tag{3.2}$$

and by Lemma 2.2 above we get

$$\Delta(B_1) \leq \Delta,\ \ \Delta(C_1^0) \leq \Delta(C_1) \leq \Delta\,. \tag{3.3}$$

It follows from (3.1) and (3.3) that there is an isogeny from A_1' to B_1/C_1 of degree $D_1 \leq M\Delta$.

Using similar arguments we obtain an isogeny from A_2' to B_2/C_2 of degree $D_2 \leq M\Delta$. So there is an isogeny from B_2/C_2 to A_2' of degree $D_2^{2m-1} \leq (M\Delta)^{2n-1}$, and combining these with f above yields the desired isogeny from A_1' to A_2'.

Finally (3.2), (3.3) and the corresponding arguments for A_2' imply $M \leq \Delta^2$, and this completes the proof of the present lemma for $m_1 = m_2 = 1$.

In general the proof is by induction on $p = m_1 + m_2$. We have just done $p = 2$, and the induction step is an easy consequence of Lemma 3.1; for example if $m_2 \geq 2$ we obtain from B in $A_1^{m_1} \times A_2^{m_2} = A_1^{m_1} \times A_2 \times A_2^{m_2-1}$ a non-split connected abelian subvariety $\tilde{B}$ either of $A_1^{m_1} \times A_2$ or of $A_1^{m_1} \times A_2^{m_2-1}$, and by Lemma 2.2 above we have $\Delta\left(\tilde{B}\right) \leq \Delta(B)$ in both cases. This completes the proof of the present lemma.

Notice that if A_1, A_2 are elliptic curves then we must have $A_1' = A_1$, $A_2' = A_2$, and if they have polarizations corresponding to Weierstrass embeddings we deduce $M = 3$. So the desired isogeny has degree at most $9\Delta^2$. This improves upon the Isogeny Lemma of [MW1] quite substantially, since the degree of B in the Segre embedding is $d!\Delta$, where d is the dimension of B.

4. Periods

In this section we recall the main result of [MW3] and we supplement it with some estimates for periods. From now on throughout the paper, the positive constants $c_1, c_2, \ldots$ will depend only on the positive integer n.

Lemma 4.1. *For each positive integer n there is a constant κ, depending only on n, with the following property. Let A be an abelian variety of dimension at most n defined over a number field of degree at most d, and suppose there is a positive definite element r of the Néron-Severi group of A of degree 1. Then for any period ω of $\Omega(A)$ the smallest algebraic subgroup G_ω of A whose tangent space contains ω satisfies*

$$\Delta(G_\omega) \leq c_1(\max\{d, h(A), r(\omega)\})^\kappa$$

Proof: Apart from the dependence on d, this is the main theorem of [MW3] in the principally polarized case. The dependence on d follows from the calculations in section 11, and we can also take for example $\kappa = (n-1)4^n n!$.

To estimate the quantities $r(\omega)$ we shall need the following result.

Lemma 4.2. *Let A be an abelian variety of dimension at most n defined over a number field of degree at most d, and suppose there is a positive definite element r of the Néron-Severi* *group of A of degree 1. Then for any algebraic subgroup B of A of positive dimension m we can find basis elements $\omega_1, \ldots, \omega_{2m}$ of $\Omega(B)$ satisfying*

$$r(\omega_i) \leq c_2(dh)^{2m-1}\Delta^2 \quad (1 \leq i \leq 2m)$$

where

$$h = \max\{1, h(A)\}, \qquad \Delta = \Delta(B)\,.$$

<u>Proof:</u> Using Lemma 2.1 [MW3] and Minkowski's Second Theorem in the geometry of numbers (see for example [C] p. 203) we can find elements $\omega_1, \ldots, \omega_{2m}$ of $\Omega(B)$, linearly independent over the rationals, such that

$$r(\omega_1)\ldots r(\omega_{2m}) \leq c_3\Delta^2\,. \tag{4.1}$$

A standard procedure (see Lemma 8, p. 135 of [C]) allows us to assume that $\omega_1, \ldots, \omega_{2m}$ actually generate $\Omega(B)$, at the expense of slightly increasing the constant in (4.1). Now it suffices to show that

$$r(\omega) \geq c_4^{-1}(dh)^{-1} \tag{4.2}$$

for any $\omega \neq 0$ in $\Omega(A)$, and this we proceed to do.

By Lemma 5.2 of [MW3] there is τ in the standard fundamental domain of the Siegel half-space, and an isomorphism f from A to the corresponding abelian variety A_τ. Further A_τ is defined over a field of degree $d_\tau \leq c_5 d$, and its canonical Riemann form r_τ satisfies $f^*(r_\tau) = r$. Hence $r(\omega) = r_\tau(\omega_\tau)$ for the period $\omega_\tau = f_*(\omega)$, and it is enough to prove (4.2) for $r_\tau(\omega_\tau)$. Let y be the imaginary part of τ, so that r_τ is represented by $zy^{-1}\bar{z}^t$ with respect to the canonical coordinates. Now the arguments in the proof of Lemma 4.1 (p. 121) of [M] show that

$$r_\tau(\omega_\tau) \geq c_6^{-1} \mid y \mid^{-1}$$

for any non-zero period ω_τ of $\Omega(A_\tau)$, where $\mid y \mid$ denotes the supremum norm of y. Throwing away all but one of the terms in the inequality of Lemma 9.6 of [MW3], we see that

$$\mid y \mid \leq c_7 d_\tau \max\{1, h(O_\tau)\}\,,$$

where $h(O_\tau)$ is the absolute logarithmic Weil height of the origin of A_τ. Finally using inequality (8.4) of [MW3] to relate $h(O_\tau)$ to $h(A_\tau) = h(A)$, we end up with the desired estimate (4.2). This proves the present lemma.

5. Preliminary isogeny estimates

In this section we start the machinery for estimating isogenies. Throughout, A_1, A_2 will be principally polarized abelian varieties of dimensions at most n, and, as before, degrees of algebraic subgroups of products $A_1^{m_1} \times A_2^{m_2}$ will be measured with respect to fixed Riemann forms r_1, r_2 on A_1, A_2 of degree 1.

Let $K = K(n)$ be the maximum of the values of the constant κ of Lemma 4.1 when the dimension in that lemma does not exceed $N = n(2n+1)$; for example $K = (N-1)4^N N!$.

Lemma 5.1. *Suppose A_1, A_2 are defined over a number field of degree at most d, and let B_1, B_2 be isogenous abelian subvarieties of A_1, A_2, of positive dimensions. Then there are abelian subvarieties B_1', B_2' of B_1, B_2, of positive dimensions, and an isogeny f' from B_1' to B_2', such that the quantities*

$$M = \max\{\Delta(B_1), \Delta(B_2)\}, \quad M' = \max\{\Delta(B_1'), \Delta(B_2')\}$$

satisfy

$$M' \leq c_1\, T^{8nK} M^{4K}$$

for

$$T = \max\{d, h(A_1), h(A_2)\},$$

and f' has degree at most $c_1\, T^{24n^2K} M^{12nK}$.

Proof: Let m be the dimension of B_1, B_2. By Lemma 4.2 we can find $\omega_0 \neq 0$ in $\Omega(B_1)$ and basis elements $\omega_1, \ldots, \omega_{2m}$ of $\Omega(B_2)$ such that

$$r_1(\omega_0) \leq c_2 T^{4n} M^2, \quad r_2(\omega_i) \leq c_2 T^{4n} M^2 \quad (1 \leq i \leq 2m).$$

Applying Lemma 4.1 to the period $\omega = (\omega_0, \omega_1, \ldots, \omega_{2m})$ of the abelian variety $A = A_1 \times A_2^{2m}$, we find that the smallest algebraic subgroup B of A whose tangent space contains ω satisfies

$$\Delta = \Delta(B) \leq c_3 T^{4nK} M^{2K}. \tag{5.1}$$

Clearly B is connected, and contained in $B_1 \times B_2^{2m}$. We claim that it is non-split with respect to B_1, B_2^{2m}. By hypothesis there is an isogeny f from B_1 to B_2, and so

$$f_*(\omega_0) = s_1\omega_1 + \ldots + s_{2m}\omega_{2m}$$

for rational integers $s_1, \ldots, s_{2m}$. Therefore B lies in the algebraic subgroup of $B_1 \times B_2^{2m}$ defined as the set of $(a_0, a_1, \ldots, a_{2m})$ satisfying

$$f(a_0) = s_1 a_1 + \ldots + s_{2m} a_{2m}.$$

Since f is an isogeny, it follows easily that if $B = H_1 \times H_2$ for H_1 in B_1, H_2 in B_2^{2m} then $H_1 = 0$; on the other hand this is impossible since $\omega_0 \neq 0$. Hence indeed B is non-split.

We may therefore apply Lemma 3.2, which yields at once the desired B_1', B_2' and f'; they satisfy the required estimates because of (5.1). This completes the proof of the present lemma.

For the fixed integer n as above we define integers $\tau(0), \tau(1), \ldots$ and $\mu(0), \mu(1), \ldots$ by the recursion rules

$$\tau(0) = \mu(0) = 0$$

and

$$\begin{aligned} \tau(m) &= 56n^2K + \tau(m-1) + 8nK\mu(m-1) \\ \mu(m) &= 28nK + (4K+1)\mu(m-1). \end{aligned} \quad (m \geq 1) \tag{5.2}$$

Lemma 5.2. *Suppose A_1, A_2 are defined over a number field of degree at most d, and let B_1, B_2 be isogenous abelian subvarieties of A_1, A_2 of dimension m. Then there is an isogeny f from B_1 to B_2 of degree at most $c_4 T^{\tau(m)} M^{\mu(m)}$, where*

$$M = \max\{\Delta(B_1), \Delta(B_2)\}, \quad T = \max\{d, h(A_1), h(A_2)\}$$

Proof: This will be by induction on m, the case $m = 0$ being trivial. We suppose that the result has been established for dimensions strictly less than m, and we proceed to deduce it for $m \geq 1$. By Lemma 5.1 there are abelian subvarieties B_1', B_2' of B_1, B_2, of positive dimensions m', and an isogeny f' from B_1' to B_2', such that

$$M' = \max\{\Delta(B_1'), \Delta(B_2')\}$$

satisfies

$$M' \leq c_5 T^{8nK} M^{4K} \tag{5.3}$$

and f' has degree

$$D' \leq c_5 T^{24n^2 K} M^{12nK}. \tag{5.4}$$

If $m' = m$ then $B_1' = B_1$, $B_2' = B_2$ and so we can take $f = f'$. Hence from now on we assume $m' < m$. Let B_1'', B_2'' be the orthogonal complements of B_1', B_2' in B_1, B_2 respectively. By Lemma 2.3 of [MW3], the quantity

$$M'' = \max\{\Delta(B_1''), \Delta(B_2'')\}$$

satisfies

$$M'' \leq MM'. \tag{5.5}$$

Since there are isogenies between B_1, B_2 and also between B_1', B_2', it follows that B_1'', B_2'' are isogenous, and we can apply the induction hypothesis. We obtain an isogeny f'' from B_1'' to B_2'' of degree

$$D'' \leq c_6 T^{\tau} (M'')^{\mu}, \tag{5.6}$$

where $\tau = \tau(m - m')$, $\mu = \mu(m - m')$. Combining f' and f'', we derive an isogeny from $B_1' \times B_1''$ to $B_2' \times B_2''$ of degree $D = D'D''$. Finally by Lemma 2.4 of [MW3] there are isogenies f_i from $B_i' \times B_i''$ to B_i of degrees

$$D_i \leq \Delta^2(B_i') \leq (M')^2 \qquad (i = 1, 2). \tag{5.7}$$

We thus end up with an isogeny f from B_1 to B_2 of degree $D_1^{2m-1} D D_2$. Using the estimates (5.3), (5.4), (5.5), (5.6) and (5.7), together with the recursion rules (5.2) and the inequalities $\tau \leq \tau(m-1)$, $\mu \leq \mu(m-1)$, we easily verify the desired upper bound for the degree of f. This completes the proof of the present lemma.

6. Proof of Theorem

We do this first when A, A^* are principally polarized. We use Lemma 5.2 with $B_1 = A_1 = A$, $B_2 = A_2 = A^*$, so that $M = 1$. We obtain an isogeny f from A to A^* of degree

$$D \leq c_1 T^\tau \tag{6.1}$$

where $\tau = \tau(n)$ and

$$T = \max\{d, h(A), h(A^*)\}.$$

To eliminate $h(A^*)$ let D_0 be the least degree of any isogeny from A to A^*. By equation (8.2) of [MW3] we deduce

$$h(A^*) \leq h(A) + \frac{1}{2}\log D_0 .$$

Putting this into (6.1) and noting that $D_0 \leq D$, we get

$$D_0 \leq c_1\left(d + h + \frac{1}{2}\log D_0\right)^\tau$$

for $h = \max\{1, h(A)\}$, and this gives easily

$$D_0 \leq c_2(d+h)^\tau . \tag{6.2}$$

This establishes our Theorem when $\delta = 1$, with $C \leq c_3 d^\tau$.

In the general case we know from Lemma 5.3 of [MW3] that there are principally polarized A_1, A_1^* and isogenies from A to A_1, A^* to A_1^* of degrees D, $D^* \leq \sqrt{\delta}$; further A_1, A_1^* are defined over a number field of degree $d_1 \leq c_4\delta^{2n}d$. So by the case (6.2) already done there is an isogeny from A_1 to A_1^* of degree

$$D_1 \leq c_5(d_1 + h_1)^\tau ,$$

where $h_1 = \max\{1, h(A_1)\}$. Hence we end up with an isogeny f from A to A^* of degree $DD_1(D^*)^{2n-1}$, and using the above inequalities together with

$$h_1 \leq h + \frac{1}{2}\log D$$

we find that f has degree at most $c_6\delta^n(\delta^{2n}d + h)^\tau$. This establishes our Theorem in general, with the exponent $\kappa = \tau$ and a constant C of the form

$$C \leq c_7 d^\tau \delta^{(2\tau+1)n} .$$

Our exponent τ is rather large. The solutions of (5.2) are

$$\tau(m) = 14n^2\{(4K+1)^m - 1\}$$
$$\mu(m) = 7n\{(4K+1)^m - 1\},$$

and so we have $\tau = \tau(n) < 14n^2(4K+1)^n$; using the value of K in section 5 we see that the Theorem holds for

$$\kappa = 14n^2\left(4N.4^N N!\right)^n, \quad N = n(2n+1).$$

For $n = 1$ this is 64512, and for $n = 2$ it exceeds 10^{30}. But of course we have been very clumsy in our induction proofs, and in [MW1] we could obtain $\kappa = 4$ for $n = 1$, so large improvements are certainly possible.

One might even conjecture that our Theorem is true for $\kappa = 0$. However, there is very little hope of proving this by the methods of the present paper; for example we already noted in [MW3] that the crucial Lemma 4.1 is definitely false with $\kappa = 0$.

7. Finiteness estimates

We prove here a quantitative version of Finiteness I. We need first the following elementary estimate.

Lemma 7.1. *For any positive integer m and any real number x there are at most x^m finite subgroups of $(\mathbf{Q}/\mathbf{Z})^m$ of orders at most x.*

Proof: The number of such subgroups is equal to

$$F_m(x) = \sum_{1 \le n \le x} f_m(n), \tag{7.1}$$

where $f_m(n)$ is the number of subgroups of order exactly n. By a well-known duality principle (see for example [C] p. 24), $f_m(n)$ is also the number of subgroups Γ of $\mathbf{Z}^m$ of index n. Now each such Γ has standard "lower triangular" basis elements (see for example [C] p. 13) of the form

$$\gamma_i = (d_{i1}, \ldots, d_{im}) \quad (1 \le i \le m)$$

with

$$d_{ij} = 0 \qquad (i < j)$$

and

$$0 \le d_{ij} < d_{jj} = d_j \qquad (1 \le j < m;\ i > j).$$

So for fixed $d_1, \ldots, d_m$ there is at most one choice for γ_1, at most d_1 for γ_2, at most $d_1 d_2$ for γ_3, and so on. Thus

$$f_m(n) = \sum d_1^{m-1} d_2^{m-2} \ldots d_{m-1},$$

where the sum is taken over all positive integers $d_1, \ldots, d_m$ with $d_1 \ldots d_m = n$. By (7.1), $F_m(x)$ is the same sum taken over all positive integers $d_1, \ldots, d_m$ with $d_1 \ldots d_m \le x$. Summing over $d_1 = d$ last, we get the identity

$$F_m(x) = \sum_{1 \le d \le x} d^{m-1} F_{m-1}(x/d) \quad (m \ge 2).$$

Now the desired inequality $F_m(x) \le x^m$ follows easily by induction on m, starting with the fact that $F_1(x)$ is the greatest integer not exceeding x. This completes the proof of the present lemma. Actually it is not too hard to show that $F_m(x)$ is asymptotic to $\zeta(2)\zeta(3)\ldots\zeta(m)x^m/m$ as $x \to \infty$, where ζ denotes the Riemann zeta function.

We can now prove the following result. Combined with Faltings's finiteness theorem for heights, it immediately implies Finiteness I.

Proposition. *Given positive integers n and d, there is a constant C_1, depending only on n and d, and there is a constant κ_1, depending only on n, with the following property. Suppose A is an abelian variety of dimension at most n defined over a number field k of degree at most d. Then there is a set $\mathcal{H} = \mathcal{H}(A)$ of real numbers, of cardinality at most $H = C_1(\max\{1, h(A)\})^{\kappa_1}$, such that if A^* is an abelian variety defined over k which is isogenous to A, then $h(A^*)$ belongs to $\mathcal{H}$ and $|\, h(A^*) - h(A) \,| \le \log H$.*

Proof: We use Zarhin's trick to overcome problems with polarization. Let $\hat{A}$, $\hat{A}^*$ be the abelian varieties dual to A, A^* respectively. Then

$$Z = \left(A \times \hat{A}\right)^4,\ Z^* = \left(A^* \times \hat{A}^*\right)^4$$

are principally polarized, defined over k, and also isogenous. So by our estimate (6.2) there is an isogeny f from Z to Z^* of degree at most $D = c_1(d+h)^\lambda$. Here λ is the value of τ with n replaced by $8n$, $h = \max\{1, h(Z)\}$, and c_1 depends only on n. By Lemma 7.1 there are at most $H = D^{16n}$ possibilities for the kernel F of f, and so also for $h(Z^*) = h(Z/F)$. Hence there are at most H possibilities for $h(A^*) = \frac{1}{8}\, h(Z^*)$, and the required estimate for H follows at once on noting that $h(Z) = 8h(A)$.

Finally there is also an isogeny from Z^* to Z of degree at most D^{16n-1}, and so the inequality (8.2) of [MW3] leads to

$$\mid h(Z^*) - h(Z) \mid \leq 8n \log D .$$

Dividing by 8, we get the required estimates for $\mid h(A^*) - h(A) \mid$. This completes the proof, with $\kappa_1 = 16n\lambda$ and $C_1 \leq c_2 d^{\kappa_1}$ for c_2 depending only on n.

It is rather difficult to make a rigorous comparison between our Proposition, expressed in terms of $h = \max\{1, h(A)\}$, and the analogous results of Raynaud in Chapter VII of [Sz] expressed in terms of reduction theory. However, we can attempt this on a heuristic basis. We start by rewriting the estimates of his Théorème 4.4.9 (p. 231) in simpler (though less explicit) form.

Assume first that A is $k-$semistable. Let s be the number of primes of k of bad reduction for A. Let l be the smallest rational prime such that A has good reduction at all primes of k dividing l, and let l' be any other such prime. Assume also that A^* is $k-$isogenous to A. In calculating Raynaud's estimate for the number of values of $h(A^*)$ it is permissible, and harmless, to choose l' of order $s \log s$. One then finds an upper bound of the shape $\exp\left(l^{C_2} \log(s+2)\right)$, where C_2 depends only on n and d. But in the estimates for $h(A^*) - h(A)$ it is perhaps better to leave l' undetermined; the upper bound now takes the form $s\left(l^{C_3} + C_3 \log l' + C_3 \log \mid \mathcal{D} \mid\right)$, where $\mathcal{D}$ is the discriminant of k, and again C_3 depends only on n and d.

In principle the above assumptions that A is $k-$semistable and A^* is $k-$isogenous to A can be removed simply by replacing k by an extension whose relative degree is bounded only by a function of n. This does not change the shape of the first estimate. However, it may not be so easy to control the discriminant in the second estimate; and indeed $\log \mid \mathcal{D} \mid$ is likely to be of order h. So for the purposes of the present comparison we restrict ourselves to semistability and isogenies over a fixed field k.

There are now two extreme situations. At one end we might have $s = 0$, $l = 2$, and then Raynaud's bounds are much better than ours. At the other end, it could be necessary to take l and l' of order h and s of order $h/\log h$; and now Raynaud's bounds are much worse than ours. Somewhere in the middle, for an abelian variety A "selected at random", one might expect $l < l' \leq f(h)$ for any function f tending to infinity, and s of order $\log h$. In this case one bound is better, the other worse than ours.

References.

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

[F] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), 349–366; and ibid., 75 (1984), p. 381.

[L] S. Lang,

[M] D.W. Masser, Small values of heights on families of abelian varieties, Diophantine approximation and transcendence theory (ed. G. Wüstholz), Lecture Notes in Math. Vol. 1290, Springer-Verlag 1987 (pp. 109–148).

[MW1] D.W. Masser and G. Wüstholz, Estimating isogenies on elliptic curves, Invent. 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, H. Lange), Lecture Notes in Math. Vol. 1399, Springer-Verlag 1989 (pp. 103–109).

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

[Se] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972), 259–331.

[Sz] L. Szpiro, Séminaire sur les pinceaux arithmétiques; la Conjecture de Mordell, Astérisque 127 (1985).