PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

D. W. MASSER
G. WÜSTHOLZ

Factorization estimates for abelian varieties

Publications mathématiques de l'I.H.É.S., tome 81 (1995), p. 5-24
<http://www.numdam.org/item?id=PMIHES_1995__81__5_0>

FACTORIZATION ESTIMATES FOR ABELIAN VARIETIES

by D. W. MASSER *and* G. WÜSTHOLZ

To Wolfgang Schmidt, with respect and admiration, on the occasion of his 60th birthday.

1. Introduction

Let A be an abelian variety. It is well-known that there exists an isogeny between A and a product $A_1^{e_1} \times \ldots \times A_t^{e_t}$, where $e_1, \ldots, e_t$ are positive integers and $A_1, \ldots, A_t$ are simple abelian varieties that are mutually non-isogenous. See for example [La] p. 30 or [Mu] p. 174. One purpose of the present article is to prove a quantitative version of this "factorization" property when A is defined over the field of algebraic numbers. For example, we shall give an estimate for the degree of the connecting isogeny.

At the same time we shall solve an apparently more general problem about isogenies. If now A and A^* are abelian varieties, defined over the field of algebraic numbers, that are isogenous, we showed in [MW3] and [MW4] how to estimate the degree of some isogeny between them. But the upper bound depended on knowing polarizations on A and A^*. The other purpose of this article is to eliminate the dependence on the polarizations.

To state our results more precisely we use the logarithmic absolute semistable Faltings height $h(A)$ of an abelian variety A defined over the field of algebraic numbers; see for example [MW2]. We work over a number field k, and we introduce an extra field K containing k in order to treat the "relative case" over K. The most interesting examples are then $K = k$ itself (the "rational case") and $K = \bar{k}$ the algebraic closure of k (the "absolute case"). The factorization estimate can now be expressed as follows.

Theorem I. — Given positive integers n and d, there is a constant κ *depending only on n, and there is a constant* C *depending only on n and d, with the following property. Suppose* A *is an abelian variety of dimension n defined over a number field k of degree d. Let* K *be any field containing k. Then there are positive integers* $e_1, \ldots, e_t$ *and abelian subvarieties* $A_1, \ldots, A_t$ *of* A, *defined over* K, *simple over* K, *and mutually non-isogenous over* K, *together with an isogeny over* K *from* A *to* $A_1^{e_1} \times \ldots \times A_t^{e_t}$ *of degree at most* $C(\max\{1, h(A)\})^{\kappa}$.

Although this result gives only a bound for the degree N of the isogeny, it is easy to deduce rather more about the factorization. Since $A_1, \ldots, A_t$ are abelian subvarieties of A it follows immediately from Lemma 2.2 (p. 414) of [MW2] (see also Lemma 7.2

below) that they are defined over an extension of k whose relative degree is bounded by an explicit function of n. Furthermore if $A^* = A_1^{e_1} \times \ldots \times A_t^{e_t}$ then it is well-known (see for example (7.2) on p. 436 of [MW2]) that

$$h(A^*) \leqslant h(A) + \frac{1}{2} \log N. \tag{1.1}$$

Since also

$$h(A^*) = e_1 h(A_1) + \ldots + e_t h(A_t) \tag{1.2}$$

and the terms on the right are bounded below (see for example (7.3) on p. 436 of [MW2]) we derive upper bounds of the form

$$\max\{h(A_1), \ldots, h(A_t)\} \leqslant C_0 \max\{1, h(A)\}$$

for C_0 depending only on n and d. Now there are up to isomorphism over $\bar{k}$ only finitely many abelian varieties defined over a number field of bounded degree with bounded dimension and bounded height. Thus we see that Theorem I could be regarded as a step towards a complete algorithm for factorization.

Next, our new isogeny estimate can be stated as follows.

Theorem II. — Given positive integers n and d, there is a constant κ depending only on n, and there is a constant C depending only on n and d, with the following property. Suppose A and A^* are abelian varieties of dimension n defined over a number field k of degree d. Let K be any field containing k. Then if they are isogenous over K, there is an isogeny over K from A to A^* of degree at most $C(\max\{1, h(A)\})^\kappa$.

Actually Theorem II implies Theorem I. For some factorization of A exists, and it is easy to see that we can suppose the factors $A_1, \ldots, A_t$ to be abelian subvarieties of A. Then $A^* = A_1^{e_1} \times \ldots \times A_t^{e_t}$ is defined over K, and we simply apply Theorem II to this situation. However, we prefer to state the two results separately, and in fact we will end up by deducing Theorem II from Theorem I through an intermediate result (see section 7).

Recall that in [MW3] and [MW4] we proved a weaker version of Theorem II in which the constant C was allowed to depend on the degrees of given polarizations on A and A^*. So the polarization hypotheses are now eliminated.

In fact we can go further and apply our methods back to the study of polarizations themselves. We shall discuss this in more detail later in section 7, but meanwhile we record here an easy consequence of Theorem II.

Corollary. — Given positive integers n and d, there is a constant κ depending only on n, and there is a constant C depending only on n and d, with the following property. Suppose A is an abelian variety of dimension n defined over a number field k of degree d. If A has only trivial endomorphisms over k, then it has a polarization defined over k of degree at most $C(\max\{1, h(A)\})^\kappa$.

Let us now make some comments about our proofs of these results.

In the context of the finiteness theorems of Faltings [F] the well-known "trick" of Zarhin [Z1] (see also [Z2]) was devised also for the purpose of removing certain polarization hypotheses. This trick has to be supplemented by the classical finiteness theorem of Jordan-Zassenhaus applied to appropriate endomorphism rings.

Naturally in our context Zarhin's trick remains indispensable. But we have already seen in [MW3] (for example the Proposition p. 470) that our considerations can lead to quantitative versions of Faltings's results. So it is not surprising that we will require for the present work a version of Jordan-Zassenhaus that is quantitative in a similar sense. However, there seem to be fundamental difficulties with proving such a result in complete generality; for example any appeal to Wedderburn's Structure Theorem is ruled out because of the use of Zorn's Lemma in constructing minimal left ideals. See also [Ro] for an interesting discussion. Of course the structure of the endomorphism ring of an abelian variety A is governed by the factorization of A into simple components (see [Mu] p. 174); but it is precisely this kind of factorization that we wish to investigate in Theorem I!

The circular argument here can be avoided by a device in section 7 later; but still it is necessary to quantify Jordan-Zassenhaus for division algebras (corresponding to simple abelian varieties). We do this in sections 2 and 3 below, obtaining rather precise bounds through the use of the geometry of numbers and the theory of cyclic algebras. The bounds are for certain "class indices", instead of the more familiar class numbers, and they are expressed in terms of discriminants. Similar (but not quite the same) indices were discussed by Bertrand [B].

These class indices arise in two different situations, both described in section 4. First, the Jordan-Zassenhaus Theorem was used by Zarhin [Z1] specifically in connexion with his concept of "stably isogenous" abelian varieties, and in Lemma 4.1 we give a quantitative version of his observation. Secondly, class indices occur in our Lemma 4.2, which also allows us to estimate certain isogenies. Some of these topics were also treated, for similar purposes, by Bertrand [B].

The statement of our Lemma 4.2 also involves an expression which for want of a better word we call a "cross-discriminant"; it appears later in section 5 as a cross-term in evaluating certain discriminants. Also in this section we recall the "Rosati discriminants" of [MW4], and we show how they are related to the usual algebra discriminants.

In section 6 we go to the number field case, and we give estimates for discriminants and cross-discriminants in terms of Faltings heights. These are deduced quite quickly from the work of [MW4]; they enable us to generalize and make explicit the estimates of section 4 for certain "product" abelian varieties.

Similarly in section 7 we use the work of [MW4] to prove a weaker form of Theorem II for such product abelian varieties, with $K = k$. From this we can deduce Theorem I, also with $K = k$, quite quickly by means of "logarithmic comparison";

and then the general version of Theorem II with $K = k$. After that we show how the results can be extended to arbitrary K. Then we prove the Corollary and add some further remarks about "estimating polarizations". Finally we discuss in more detail the constants C and κ.

The first author was partially supported by a grant from the National Science Foundation. He would also like to thank the Alexander von Humboldt Foundation for additional support, and the University of Konstanz for friendly hospitality. This paper also profited from several remarks of D. Bertrand and J. T. Stafford; in particular the former sharpened our original inequality of Lemma 5.2 to an equality, and the latter improved our original version of Lemma 2.2.

2. The class index

Let $\mathcal{O}$ be an order. By this we mean that $\mathcal{O}$ is a ring, containing a multiplicative identity, which is free and finitely generated as an additive group. Thus $D = \mathcal{O} \otimes \mathbf{Q}$ is a $\mathbf{Q}$-algebra; let m be its dimension over $\mathbf{Q}$.

Let tr denote the (non-reduced) trace from D to $\mathbf{Q}$ obtained as in [Re] (p. 3) from the left regular representation. A lattice Λ in D is simply an additive subgroup of D of $\mathbf{Z}$-rank m, and we define the discriminant $d(\Lambda)$ as the determinant of the $\mathrm{tr}(\lambda_i \lambda_j)$ $(1 \leqslant i, j \leqslant m)$ for any choice of elements $\lambda_1, \ldots, \lambda_m$ in a $\mathbf{Z}$-basis for Λ. This is independent of the basis elements. Since D is separable ([Re] p. 99), it follows easily that $d(\Lambda)$ is non-zero (compare [Re] p. 126), and we note the obvious relation

$$d(\tilde{\Lambda}) = [\Lambda : \tilde{\Lambda}]^2 \, d(\Lambda) \tag{2.1}$$

for any sublattice $\tilde{\Lambda}$ of Λ with index $[\Lambda : \tilde{\Lambda}]$.

Now suppose D is a division algebra, and let e be a positive integer. We define the (left) class index $i_e(\mathcal{O})$ of the order $\mathcal{O}$ as the smallest positive integer I such that every torsion-free left $\mathcal{O}$-module of $\mathcal{O}$-rank e contains a free submodule of index not exceeding I. The finiteness of $i_e(\mathcal{O})$ is a very special case of the celebrated Jordan-Zassenhaus Theorem (see for example [Re] p. 228 or [CR1] p. 559 or [CR2] p. 534).

The main result of the present section, the Class Index Lemma, provides a simple estimate for $i_e(\mathcal{O})$ in terms of the discriminant $d(\mathcal{O})$.

Class Index Lemma. — For any order $\mathcal{O}$ in a division algebra as above, and any positive integer e, we have

$$i_e(\mathcal{O}) \leqslant |\, d(\mathcal{O}) \,|^{e/2}.$$

If $\mathcal{O}$ is the ring of integers of a number field and $e = 1$, this estimate is classical (see for example [H] p. 608). Our proof generalizes the classical proof in a sequence of lemmas. We start with another definition.

Let Λ be a lattice in D, and choose elements $\lambda_1, \ldots, \lambda_m$ in a $\mathbf{Z}$-basis for Λ. If nm is

the norm (again see [Re] p. 3) from D to $\mathbf{Q}$, extended to $D \otimes \mathbf{R}$, then the set $\mathscr{S}$ of all $(s_1, \ldots, s_m)$ in $\mathbf{R}^m$ satisfying

$$|\, nm(s_1 \lambda_1 + \ldots + s_m \lambda_m)\,| \leqslant 1 \tag{2.2}$$

is clearly a symmetric set containing a neighbourhood of the origin. It is sometimes, but not always, convex. But there are always convex symmetric sets $\mathscr{S}_0$ of positive volume contained in $\mathscr{S}$, and it is not difficult to see that the volumes of such sets are bounded from above (for example this is implicit in the proof of Lemma 2.1 below). Furthermore the supremum of these volumes depends only on Λ and not on the choice of basis elements $\lambda_1, \ldots, \lambda_m$. If $v(\Lambda)$ denotes this supremum, we also have

$$v(\widetilde{\Lambda}) = [\Lambda : \widetilde{\Lambda}]^{-1}\, v(\Lambda) \tag{2.3}$$

for any sublattice $\widetilde{\Lambda}$ of Λ.

Now consider the product $p(\Lambda) = |\, d(\Lambda)\,|^{1/2}\, v(\Lambda)$. Comparing (2.1) and (2.3) we see that $p(\widetilde{\Lambda}) = p(\Lambda)$ for every sublattice $\widetilde{\Lambda}$ of Λ. Since any two sublattices have a common sublattice, it follows that $p(\Lambda)$ is independent of Λ, and so it depends only on the ambient division algebra D. So we can denote it by $p(D)$ instead.

The following result is a preliminary estimate for the class index when $e = 1$.

Lemma **2.1.** — *We have*

$$i_1(\mathscr{O}) \leqslant 2^m\, |\, d(\mathscr{O})\,|^{1/2} / p(D).$$

Proof. — This imitates the arguments in [Re] (p. 227, 228), except that the Box Principle is replaced by the more precise Geometry of Numbers, as in the classical treatment of class numbers.

Let M be an arbitrary torsion-free left $\mathscr{O}$-module of $\mathscr{O}$-rank 1. Replacing M by an $\mathscr{O}$-isomorphic copy, we can suppose that it is a submodule of $\mathscr{O}$ itself. Pick any elements $\varepsilon_1, \ldots, \varepsilon_m$ of a $\mathbf{Z}$-basis of $\mathscr{O}$; then the set of $(n_1, \ldots, n_m)$ in $\mathbf{Z}^m$ such that $n_1 \varepsilon_1 + \ldots + n_m \varepsilon_m$ belongs to M is a lattice in $\mathbf{Z}^m$ (in the Minkowski sense), whose determinant is $N = [\mathscr{O} : M]$.

Choose any real $T > 2^m\, N / v(\mathscr{O})$. Then $v(\mathscr{O}) > 2^m\, N/T$, so by definition there is a convex symmetric set $\mathscr{S}_0$ in $\mathbf{R}^m$, with volume bigger than $2^m\, N/T$, such that (2.2) holds for every $(s_1, \ldots, s_m)$ in $\mathscr{S}_0$. Now the scaled set $T^{1/m}\, \mathscr{S}_0$ has volume bigger than $2^m\, N$, and so by Minkowski's First Theorem (see for example [Ca] p. 72) it contains a non-zero lattice point. This gives $\mu = n_1 \varepsilon_1 + \ldots + n_m \varepsilon_m \neq 0$ in M with

$$|\, nm\, \mu\,| \leqslant T. \tag{2.4}$$

Now $\mathcal{O}\mu$ is a free submodule of M of index $[\mathcal{O} : \mathcal{O}\mu]/N$. But it is well-known that $[\mathcal{O} : \mathcal{O}\mu] = |\, nm\, \mu\,|$ (see for example [CR1] p. 127), so we conclude from (2.4) that $i_1(\mathcal{O}) \leqslant T/N$. Since this is any number bigger than $2^m/v(\mathcal{O}) = 2^m \mid d(\mathcal{O})|^{1/2}/p(D)$, and M was arbitrary, the proof of Lemma 2.1 is thereby complete.

Now if $\mathcal{O}$ is a Dedekind domain it is classical that $i_e(\mathcal{O}) = i_1(\mathcal{O})$ for every positive integer e (see for example [Ca] p. 110 or § 22 of [CR1], especially p. 155). Stafford pointed out that the same is true even if $\mathcal{O}$ is a "non-commutative Dedekind domain"; for example a maximal order in D. In general we can prove the following result.

Lemma **2.2.** — *For any integer* $e \geqslant 2$ *we have*

$$i_e(\mathcal{O}) \leqslant i_1(\mathcal{O})\, i_{e-1}(\mathcal{O}).$$

Proof. — We are grateful to Stafford for this argument. Let M be an arbitrary torsion-free left $\mathcal{O}$-module of $\mathcal{O}$-rank e. Replacing M by an $\mathcal{O}$-isomorphic copy, we can suppose that it is a submodule of $\mathcal{O}^e$. By projecting to a fixed coordinate we obtain an exact inclusion-projection sequence

$$0 \to \mathcal{O}^{e-1} \to \mathcal{O}^e \to \mathcal{O} \to 0,$$

and restricting to M gives another exact sequence

$$0 \to M_0 \to M \to M_1 \to 0,$$

where $M_0 = \mathcal{O}^{e-1} \cap M$ and $M_1 = \pi(M)$ for the projection π. Now there is μ_1 in M_1 and a free submodule $\widetilde{M}_0$ of M_0 such that

$$\textbf{(2.5)} \qquad [M_1 : \mathcal{O}\mu_1] \leqslant i_1(\mathcal{O}), \quad [M_0 : \widetilde{M}_0] \leqslant i_{e-1}(\mathcal{O}).$$

Pick μ in M with $\pi(\mu) = \mu_1$; it is easy to see that $M' = M_0 + \mathcal{O}\mu$ is a direct sum, and that M/M' is isomorphic to $M_1/\mathcal{O}\mu_1$. In particular $[M : M'] = [M_1 : \mathcal{O}\mu_1]$. Also for $\widetilde{M} = \widetilde{M}_0 + \mathcal{O}\mu$ we have $[M' : \widetilde{M}] = [M_0 : \widetilde{M}_0]$, so that (2.5) leads to

$$[M : \widetilde{M}] = [M : M']\,[M' : \widetilde{M}] \leqslant i_1(\mathcal{O})\, i_{e-1}(\mathcal{O}).$$

Since M was arbitrary, and $\widetilde{M}$ is free, the assertion of the present lemma follows at once.

It is now clear that the Class Index Lemma can be proved by induction from the above two results, provided we can establish the lower bound

$$\textbf{(2.6)} \qquad p(D) \geqslant 2^m.$$

This will be done in the next section.

Finally it may be interesting to compare the class index $i_1(\mathcal{O})$ with the more conventional class number $h(\mathcal{O})$ that counts $\mathcal{O}$-isomorphism classes of left $\mathcal{O}$-modules of $\mathcal{O}$-rank 1. For example, using Lemma 6.1 (p. 469) of [MW3] we find easily that $h(\mathcal{O}) \leqslant (i_1(\mathcal{O}))^m$. But it is not clear whether conversely $i_1(\mathcal{O})$ can be bounded above in terms of $h(\mathcal{O})$.

3. Cyclic algebras

In Lemma 3.3 below we will establish (2.6) for any finite-dimensional division algebra D over $\mathbf{Q}$.

Our proof makes essential use of the Albert-Brauer-Hasse-Noether Theorem, or rather its consequence that D is cyclic over its centre F (see for example [P] p. 359). Now F is a number field, and this means that there is a Galois extension E of F, with cyclic group generated by σ, say, together with a non-zero element a of F such that $D = (E, \sigma, a)$ in the notation of [P] (p. 277). If the relative degree $[E : F]$ is n, then

$$D = E \oplus uE \oplus \ldots \oplus u^{n-1} E,$$

where $u^n = a$ and

$$cu = uc^{\sigma} \tag{3.1}$$

for all c in E.

We will need some formulae for trace and norm; these come most conveniently from the left regular representation over E. Then for $c_0, \ldots, c_{n-1}$ in E the corresponding element

$$x = c_0 + uc_1 + \ldots + u^{n-1} c_{n-1} \tag{3.2}$$

in D is represented by the matrix $M(x)$ with entries $m_{ij} = m_{ij}(x)$ $(0 \leqslant i, j \leqslant n-1)$ given by

$$\begin{cases} m_{ij} = c_{i-j}^{\sigma^j} & (i \geqslant j) \\ m_{ij} = a c_{i-j+n}^{\sigma^j} & (i < j) \end{cases} \tag{3.3}$$

(see [P] p. 298). Thus

$$\mathrm{tr}_{D/E}(x) = \mathrm{Tr}\, M(x) = \mathrm{tr}_{E/F}(c_0)$$

and

$$nm_{D/E}(x) = \mathrm{Det}\, M(x)$$

for the standard matrix Tr and Det. The traces and norms over F are appropriate multiples and powers respectively (see [P] p. 295), and those over $\mathbf{Q}$ are obtained by taking conjugates (see [Re] p. 119). We end up with

$$\mathrm{tr}\, x = n\, \mathrm{tr}_{E/\mathbf{Q}}(c_0) \tag{3.4}$$

$$nm\, x = \{ nm_{F/\mathbf{Q}}(\mathrm{Det}\, M(x)) \}^n. \tag{3.5}$$

Note that $m = n^2 d$, where d is the degree $[F : \mathbf{Q}]$ of F.

We define the lattice

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \ldots \oplus u^{n-1} \mathcal{O}_E,$$

where $\mathcal{O}_E$ is the ring of integers of E.

Lemma **3.1.** — *We have*

$$| d(\Lambda)| = n^{nr} \mid d(\mathcal{O}_{\mathrm{E}})|^{n} \mid nm_{\mathrm{F/Q}}(a)|^{n(n-1)},$$

where $r = nd$ *is the degree of* E, *and* $d(\mathcal{O}_{\mathrm{E}})$ *is the field discriminant.*

Proof. — Choose elements $e_1, \ldots, e_r$ of a **Z**-basis of $\mathcal{O}_{\mathrm{E}}$. Using (3.2) to write down the obvious **Z**-basis of Λ, we find that the matrix defining $d(\Lambda)$ breaks into blocks as

$$\begin{bmatrix} \mathrm{M}_0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & \mathrm{M}_{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \mathrm{M}_1 & \ldots & 0 \end{bmatrix}$$

where M_0 has entries tr $(e_p e_q)$ and M_i $(1 \leqslant i \leqslant n-1)$ has entries tr $(ae_p^{\sigma^i} e_q)$ $(1 \leqslant p, q \leqslant r)$. So

$$d(\Lambda) = \pm (\mathrm{Det}\ \mathrm{M}_0) \prod_{i=1}^{n-1} (\mathrm{Det}\ \mathrm{M}_i). \tag{3.6}$$

By (3.4) we see that

$$\mathrm{Det}\ \mathrm{M}_0 = n^r\, d(\mathcal{O}_{\mathrm{E}}). \tag{3.7}$$

Also by considering the left regular representation of a in E, and noting that σ^i has action with determinant ± 1, we find that

$$\mathrm{Det}\ \mathrm{M}_i = \pm n^r\, d(\mathcal{O}_{\mathrm{E}})\, nm_{\mathrm{E/Q}}(a) \quad (1 \leqslant i \leqslant n-1).$$

Now Lemma 3.1 follows from this together with (3.6) and (3.7).

Next, keep some choice $e_1, \ldots, e_r$ of elements of a **Z**-basis of $\mathcal{O}_{\mathrm{E}}$. Write $\tau_1, \ldots, \tau_d$ for the different complex embeddings of F, extended in some fixed way to E. We define a set $\mathcal{S}_0$ in $\mathbf{R}^m$ as follows. A typical element λ of Λ has the form (3.2) where $c_0, \ldots, c_{n-1}$ are linear combinations of $e_1, \ldots, e_r$ with rational integer coefficients. We interpret these coefficients as coordinates in $\mathbf{R}^m$ for $\Lambda \otimes \mathbf{R}$, and we define $\mathcal{S}_0$ by the inequalities

$$| c_i^{\sigma^j \tau_k} | \leqslant \nu \mid a^{\tau_k} |^{-i/n} \quad (0 \leqslant i, j \leqslant n-1,\ 1 \leqslant k \leqslant d), \tag{3.8}$$

where $\nu = n^{-1/2}$.

Lemma **3.2.** — *The volume of* $\mathcal{S}_0$ *is*

$$\{ 2^{r_1}(2\pi)^{r_2} \}^n\, n^{-nr/2} \mid d(\mathcal{O}_{\mathrm{E}})|^{-n/2} \mid nm_{\mathrm{F/Q}}(a) |^{-n(n-1)/2},$$

where r_1 *and* $2r_2$ *are the numbers of real and non-real complex embeddings of* E *respectively.*

Proof. — The $\tau = \sigma^j \tau_k$ $(0 \leqslant j \leqslant n-1, 1 \leqslant k \leqslant d)$ are all the different complex embeddings of E, and $a^\tau = a^{\tau_k}$. So by (3.8) the volume of $\mathscr{S}_0$ is given by $\prod_{i=0}^{n-1} V_i$. Here V_i is the volume of the set in $\mathbf{R}^r$ defined by the inequalities

$$| c^\tau | \leqslant \nu | a^\tau |^{-i/n}$$

as τ varies, where now the coefficients of $e_1, \ldots, e_r$ in c are regarded as coordinates. But it is well-known (see for example [H] p. 611) that the volume of the set defined by $| c^\tau | \leqslant 1$ is

$$\mathbf{(3.9)} \qquad V = 2^{r_1}(2\pi)^{r_2} | d(\mathscr{O}_E) |^{-1/2}.$$

It follows that

$$V_i = \nu^r V | nm_{E/\mathbf{Q}}(a) |^{-i/n} \quad (0 \leqslant i \leqslant n-1).$$

Now Lemma 3.2 follows from this together with (3.9).

Lemma **3.3.** — *We have* $p(D) \geqslant 2^m$ *for any division algebra* D *of dimension* m *over* $\mathbf{Q}$.

Proof. — Clearly the set $\mathscr{S}_0$ defined by (3.8) is convex and symmetric. We will verify that if x in $D \otimes \mathbf{R}$ is given by (3.2) and satisfies (3.8), then

$$\mathbf{(3.10)} \qquad | nm\, x | \leqslant 1.$$

For fix k with $1 \leqslant k \leqslant d$. Then the entries $\xi_{ij} = m_{ij}^{\tau_k}$ in (3.3) of the matrix $M(x)^{\tau_k}$ satisfy

$$| \xi_{ij} | \leqslant \nu X^{j-i} \quad (0 \leqslant i, j \leqslant n-1)$$

with $X = | a^{\tau_k} |^{1/n}$. It follows easily from properties of determinants together with Hadamard's inequality that

$$| \mathrm{Det}\, M(x)^{\tau_k} | \leqslant \nu^n n^{n/2} = 1 \quad (1 \leqslant k \leqslant d).$$

Now (3.10) is an immediate consequence of this together with (3.5).

We deduce that the set $\mathscr{S}_0$ satisfies the conditions in the definition of $v(\Lambda)$. So $v(\Lambda)$ is no smaller than the volume of $\mathscr{S}_0$, and finally Lemmas 3.1 and 3.2 give

$$p(D) = | d(\Lambda) |^{1/2} v(\Lambda) \geqslant \{ 2^{r_1}(2\pi)^{r_2} \}^n \geqslant 2^m$$

as required. This completes the proof of the present lemma, and, as we have already observed, of the Class Index Lemma as well.

Finally we will at one point have to switch over from left to right, at least for $e = 1$. We defined the left class index $i_1(\mathscr{O})$ with reference to left $\mathscr{O}$-modules. We could also define the right class index $i_1'(\mathscr{O})$ with reference to right $\mathscr{O}$-modules. The trace is defined in [Re] (p. 3) with respect to the left regular representation but, since $D = \mathscr{O} \otimes \mathbf{Q}$ si

separable, this same trace can equally well be calculated using the right regular representation ([Re] p. 123). So we can follow the proof of the Class Index Lemma with appropriate modifications to give the same estimate

$$i_1'(\mathcal{O}) \leqslant |d(\mathcal{O})|^{1/2} \tag{3.11}$$

for the right class index.

4. Simple abelian varieties

In his paper [Z1] Zarhin introduced the concept of stable isogeny between abelian varieties, and he indicated the connexion with the Jordan-Zassenhaus Theorem. We start by making this connexion precise, in terms of the class index.

Let k be a field. For the whole of the present section we work with the "rational case"; thus all abelian varieties, abelian subvarieties, homomorphisms, endomorphisms, isomorphisms and isogenies will be assumed to be defined over k, as well as the concept of simplicity.

Recall that if A is an abelian variety, then the ring $\mathcal{O} = \mathrm{End}\, A$ of endomorphisms is an order in the sense of section 2. Also every f in $\mathcal{O}$ has a trace $\mathrm{TR}f$ and a norm $\mathrm{NM}f$ defined in terms of the characteristic polynomial (see [Mu] p. 182). Suppose A is isotypic; that is, isogenous to some power of a simple abelian variety. Then if n is the dimension of A and m is the $\mathbf{Z}$-rank of $\mathcal{O}$ we have

$$2n\,\mathrm{tr}f = m\,\mathrm{TR}f \tag{4.1}$$

$$(nmf)^{2n} = (\mathrm{NM}f)^m \tag{4.2}$$

for the trace and norm used in section 2; further if f is an isogeny then its degree $\deg f$ is just $\mathrm{NM}f$. Finally if A is itself simple, then $\mathcal{O} \otimes \mathbf{Q}$ is a division algebra, so we can use the class index estimates of sections 2 and 3.

Lemma **4.1.** — *For positive integers* n, N *and* e *let* A *be a simple abelian variety of dimension* n, *and suppose* B *is an abelian subvariety of* A^{N} *that is isogenous to* A^e. *Then there is an isogeny from* B *to* A^e *of degree at most* $(i_e(\mathcal{O}))^{2ne}$, *where* $\mathcal{O} = \mathrm{End}\, \mathrm{A}$.

Proof (compare also section 5 of [Z1] and the proof of Proposition 2 of [B], as well as [LOZ]). — By hypothesis there is φ in $\mathrm{Hom}(\mathrm{A}^e, \mathrm{A}^{\mathrm{N}})$ such that $\mathrm{B} = \varphi(\mathrm{A}^e)$. Write $\varphi = (\varphi_1, \ldots, \varphi_{\mathrm{N}})$ for $\varphi_1, \ldots, \varphi_{\mathrm{N}}$ in $\mathscr{H} = \mathrm{Hom}(\mathrm{A}^e, \mathrm{A})$. We regard $\mathscr{H}$ as a (torsion-free) left $\mathcal{O}$-module, so that $\mathrm{M} = \sum_{k=1}^{\mathrm{N}} \mathcal{O}\varphi_k$ is a left $\mathcal{O}$-module of $\mathscr{H}$. Since B is actually isogenous to A^e, it follows that M has $\mathcal{O}$-rank exactly e. Hence by the Class Index Lemma there are $\tilde{\varphi}_1, \ldots, \tilde{\varphi}_e$ in $\mathscr{H}$ such that $\tilde{\mathrm{M}} = \sum_{j=1}^{e} \mathcal{O}\tilde{\varphi}_j$ is free and contained in M, with index

$$\mathrm{I} = [\mathrm{M} : \tilde{\mathrm{M}}] \leqslant i_e(\mathcal{O}). \tag{4.3}$$

In particular, there are ε_{jk}, $\tilde{\varepsilon}_{kj}$ in $\mathcal{O}$ such that

$$\tilde{\varphi}_j = \sum_{k=1}^{N} \varepsilon_{jk} \varphi_k \quad (1 \leqslant j \leqslant e) \tag{4.4}$$

and

$$I\varphi_k = \sum_{j=1}^{e} \tilde{\varepsilon}_{kj} \tilde{\varphi}_j \quad (1 \leqslant k \leqslant N). \tag{4.5}$$

We define ψ from A^N to A^e by $\psi = (\psi_1, \ldots, \psi_e)$, where

$$\psi_j(a_1, \ldots, a_N) = \sum_{k=1}^{N} \varepsilon_{jk} a_k \quad (1 \leqslant j \leqslant e)$$

for $a_1, \ldots, a_N$ in A, and we claim that ψ restricted to B is an isogeny.

For suppose $\psi(b) = 0$ for some b in B, so that $b = \varphi(\alpha)$ for some α in A^e. It follows from (4.4) that $\tilde{\varphi}_j(\alpha) = 0$ $(1 \leqslant j \leqslant e)$, and then from (4.5) that $Ib = 0$. Thus ψ restricted to B is indeed an isogeny, and since B has dimension ne we see that the degree of this isogeny is at most I^{2ne}. In view of (4.3) this completes the proof of the present lemma.

For the next result we need a preliminary definition. Recall that D is a $\mathbf{Q}$-algebra of finite dimension. A lattice Λ in D is a free finitely generated additive subgroup of D with $\Lambda \otimes \mathbf{Q} = D$, and for this we defined the discriminant $d(\Lambda)$ in section 2. As a generalization we fix a left D-module V; then its dual $\mathrm{Hom}_D(V, D)$ is a right D-module (see [CR2] p. 610). For v in V and v' in $\mathrm{Hom}_D(V, D)$ we can define the product vv' as the image of v by v'.

Now for free finitely generated additive subgroups M, M′ of V, $\mathrm{Hom}_D(V, D)$ respectively, of the same $\mathbf{Z}$-rank ℓ, say, we consider the determinant Δ of the $\mathrm{tr}(\mu_i \mu_j')$ $(1 \leqslant i, j \leqslant \ell)$, where $\mu_1, \ldots, \mu_\ell$ and $\mu_1', \ldots, \mu_\ell'$ are choices of elements from $\mathbf{Z}$-bases of M and M′ respectively. If we change these choices, then Δ can change only in sign; thus Δ^2 is well-defined, and it is this we call the cross-discriminant $c(M, M')$ of M and M′. By analogy with (2.1), we have

$$c(\tilde{M}, \tilde{M}') = [M : \tilde{M}]^2 [M' : \tilde{M}']^2 c(M, M') \tag{4.6}$$

for any subgroups $\tilde{M}$, $\tilde{M}'$ of finite indices in M, M′ respectively.

In practice D and V will be obtained from simple isogenous abelian varieties A and B by choosing D as $\mathcal{O} \otimes \mathbf{Q}$ and V as $\mathcal{H} \otimes \mathbf{Q}$ for

$$\mathcal{O} = \mathrm{End}\, A, \quad \mathcal{H} = \mathrm{Hom}(B, A).$$

Then $\mathrm{Hom}_D(V, D)$ can be canonically identified with $\mathcal{H}' \otimes \mathbf{Q}$, where

$$\mathcal{H}' = \mathrm{Hom}(A, B),$$

and the above product coincides with composition. In the present paper we will restrict M and M′ to lattices in $\mathcal{H}$ and $\mathcal{H}'$ respectively. If $M = \mathcal{H}$ and $M' = \mathcal{H}'$ then Lemma 5.1 *b)*

below shows that the cross-discriminant can be expressed in terms of discriminants. Its usefulness in estimating isogenies is shown in the following result.

Lemma **4.2.** — *For a positive integer n let* A *be a simple abelian variety of dimension n, and suppose* B *is an abelian variety isogenous to* A. *Then there is an isogeny from* B *to* A *of degree at most* $(c(\mathscr{H}, \mathscr{H}'))^n$, *where*

$$\mathscr{H} = \mathrm{Hom}(\mathrm{B}, \mathrm{A}), \quad \mathscr{H}' = \mathrm{Hom}(\mathrm{A}, \mathrm{B}).$$

Proof. — Since $\mathscr{H}$ is a left $\mathcal{O}$-module of $\mathcal{O}$-rank 1, it contains by the Class Index Lemma η with

$$[\mathscr{H} : \mathcal{O}\eta] = \mathrm{N} \leqslant i_1(\mathcal{O}) \leqslant |\, d \,|^{1/2}, \tag{4.7}$$

where $d = d(\mathcal{O})$. Also $\mathscr{H}'$ is a right $\mathcal{O}$-module of $\mathcal{O}$-rank 1, so that, by (3.11), it contains η' with

$$[\mathscr{H}' : \eta'\,\mathcal{O}] = \mathrm{N}' \leqslant i_1'(\mathcal{O}) \leqslant |\, d \,|^{1/2}. \tag{4.8}$$

Thus from (4.6) we get

$$(\mathrm{NN}')^2\, c(\mathscr{H}, \mathscr{H}') = c(\mathcal{O}\eta, \eta'\,\mathcal{O}) = \Delta^2, \tag{4.9}$$

where Δ is the determinant of the $\mathrm{tr}(\varepsilon_i\, \delta\varepsilon_j)$ $(1 \leqslant i, j \leqslant m)$ for $\delta = \eta\eta'$ in $\mathcal{O}$. Here $\varepsilon_1, \ldots, \varepsilon_m$ are elements of any $\mathbf{Z}$-basis for $\mathcal{O}$. Now (4.7), (4.8) and (4.9) give

$$\Delta^2 \leqslant |\, d \,|^2\, c(\mathscr{H}, \mathscr{H}'). \tag{4.10}$$

On the other hand, using the left (or right) regular representation of δ, we see that $\Delta = d(nm\,\delta)$. Thus comparison with (4.10) yields

$$|\, nm\,\delta \,|^2 \leqslant c(\mathscr{H}, \mathscr{H}'). \tag{4.11}$$

Also by (4.2) we have

$$(nm\,\delta)^{2n/m} = \deg \delta = (\deg \eta)\,(\deg \eta'). \tag{4.12}$$

Finally the required estimate for the degree of the isogeny η from B to A follows from (4.11) and (4.12) after throwing away $\deg \eta'$ and using $m \geqslant 1$.

5. Discriminants

We continue to work in the "rational case" as in the preceding section; now also polarizations will be assumed to be defined over the ground field. The following result shows that our cross-discriminant can often be expressed in terms of discriminants.

Lemma **5.1.** — *a) For an isotypic abelian variety* A *we have*

$$d(\text{End } A^2) = (-1)^m 2^{4m} (d(\text{End } A))^4,$$

where m *is the* **Z***-rank of* End A.

b) Suppose further that A *is simple and* B *is isogenous to* A. *Then*

$$d(\text{End } A \times B) = (-1)^m 2^{4m} c(\mathscr{H}, \mathscr{H}')\, d(\text{End } A)\, d(\text{End } B),$$

where $\mathscr{H} = \text{Hom}(B, A), \quad \mathscr{H}' = \text{Hom}(A, B).$

Proof. — Assume for the moment only that A and B are isogenous isotypic abelian varieties of the same dimension. As in section 6 of [MW4], we express elements f of $F = \text{End } A \times B$ as matrices $\begin{bmatrix} \varepsilon & \eta \\ \eta' & \delta \end{bmatrix}$, where ε, δ, η, η' are in End A, End B, $\mathscr{H}, \mathscr{H}'$ respectively. So the **Z**-rank of F is $k = 4m$. Also $\text{TR}\, f = \text{TR}\, \varepsilon + \text{TR}\, \delta$, which from (4.1) leads to

$$\text{tr}\, f = 2\, \text{tr}\, \varepsilon + 2\, \text{tr}\, \delta \tag{5.1}$$

when the traces are normalized as in section 2. Now we can write down elements $f_1, \ldots, f_k$ of a **Z**-basis of F in the form $\begin{bmatrix} \varepsilon & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \eta \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ \eta' & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & \delta \end{bmatrix}$, and we calculate $d(F)$ with these. The resulting matrix with entries $\text{tr}(f_i f_j)$ $(1 \leqslant i, j \leqslant k)$ splits into blocks as

$$\begin{bmatrix} M_1 & M_1' & 0 & 0 \\ 0 & 0 & M_2 & M_2' \\ M_3' & M_3 & 0 & 0 \\ 0 & 0 & M_4' & M_4 \end{bmatrix}.$$

From (5.1) we find that $M_i' = 0$ as well $(1 \leqslant i \leqslant 4)$, and that the determinants $D_i = \text{Det } M_i$ $(1 \leqslant i \leqslant 4)$ satisfy

$$D_1 = 2^m d(\text{End } A), \quad D_4 = 2^m d(\text{End } B). \tag{5.2}$$

Also $\text{TR}(\eta\eta')$ in End A is the same as $\text{TR}(\eta'\eta)$ in End B, so that (4.1) gives $\text{tr}(\eta\eta') = \text{tr}(\eta'\eta)$. Now in case *b)* we find that

$$D_2 D_3 = 2^{2m} c(\mathscr{H}, \mathscr{H}') \tag{5.3}$$

whereas in case *a)* with B = A we can split the factors to get

(5.4) $$D_2 = D_3 = 2^m\, d(\mathrm{End}\ A).$$

Finally since $d(F) = (-1)^m D_1 D_2 D_3 D_4$ we deduce the required formulae from (5.2), (5.3) and (5.4); this completes the proof of the present lemma.

Next suppose A is an abelian variety defined over a subfield k of $\mathbf{C}$, and let r be a polarization of A. In [MW4] we defined the Rosati discriminant $D_r(\mathcal{O})$ as the determinant of the $\mathrm{TR}(f_i f_j^\dagger)$ $(1 \leqslant i, j \leqslant m)$, where $f_1, \ldots, f_m$ are elements of any $\mathbf{Z}$-basis of $\mathcal{O} = \mathrm{End}\ A$, and $f^\dagger$ denotes the image of f under the Rosati involution associated with r. Note here that the trace is that defined by the characteristic polynomial.

Lemma **5.2.** — *For a polarized isotypic abelian variety* A *as above we have*

$$(2n)^m\, |\, d(\mathcal{O})\, | = m^m\, D_r(\mathcal{O}),$$

where n is the dimension of A *and m is the* $\mathbf{Z}$*-rank of* $\mathcal{O} = \mathrm{End}\ A$.

Proof. — Originally we had only the corresponding upper bound for $|\, d(\mathcal{O})\,|$ (which suffices for the purpose of this paper), and we are grateful to Bertrand for pointing out that equality holds, as well as clarifying the nature of the isotypic hypothesis. For the proof one observes that the action of any involution on any $\mathbf{Z}$-basis must have determinant ± 1. The desired result follows from (4.1) on noting that $D_r(\mathcal{O}) > 0$. This completes the proof.

6. Preliminary estimates

For an abelian variety A we denote by $\hat{A}$ its dual abelian variety (see for example [Mu] p. 123, or, in zero characteristic, p. 86). We also use the notation

$$Z(A) = (A \times \hat{A})^4$$

for the abelian variety introduced by Zarhin.

Suppose A has dimension n and is defined over a number field k of degree d. We continue to work with the rational case as in the preceding two sections. Let r be a polarization on A of degree δ. The main result of [MW4] is an estimate for the Rosati discriminant $D_r(\mathcal{O})$ of $\mathcal{O} = \mathrm{End}\ A$, of the following form. Let $h(A)$ be the Faltings height of A as in section 1. Then

(6.1) $$D_r(\mathcal{O}) \leqslant C(\max\{1, h(A)\})^{\lambda(n)},$$

where $\lambda(n)$ depends only on n, and C depends only on n, d and δ. For convenience we shall suppose that $\lambda(n)$ is monotonically non-decreasing in n.

Our first task is to convert this into an estimate for the ordinary discriminant $d(\mathcal{O})$. Of course we could immediately use Lemma 5.2 for this purpose, but we need an upper

bound independent of polarizations. So we use Zarhin's trick. At the same time we estimate an associated cross-discriminant. The outcome is as follows; henceforth $c_1, c_2, \ldots$ will denote unspecified positive constants depending only on n and d.

Lemma **6.1.** — *Suppose* A *is a simple abelian variety of dimension n. Then we have*

$$\max\{\,|d(\mathcal{O})|, c(\mathscr{H}, \mathscr{H}')\} \leqslant c_1(\max\{1, h(A)\})^{\lambda(8n)},$$

where $\mathcal{O} = \mathrm{End}\, A, \quad \mathscr{H} = \mathrm{Hom}(\hat{A}, A), \quad \mathscr{H}' = \mathrm{Hom}(A, \hat{A}).$

Proof. — The abelian variety $Z = Z(A)$ is defined over the same field as A, and of course it has a principal polarization r defined over this field (though not a canonical one). Its dimension is $8n$, and $h(Z) = 8h(A)$, so that (6.1) with $\delta = 1$ gives

$$D_r(\mathrm{End}\, Z) \leqslant c_2 h^{\lambda},$$

where $h = \max\{1, h(A)\}$ and $\lambda = \lambda(8n)$. So by Lemma 5.2 we have also

(6.2) $$|d(\mathrm{End}\, Z)| \leqslant c_3 h^{\lambda}$$

for $Z = (A \times \hat{A})^4$. Now a double application of Lemma 5.1 *a)* to (6.2) shows that

$$|d(\mathrm{End}\, A \times \hat{A})| \leqslant c_4 h^{\lambda/16}.$$

Finally Lemma 5.1 *b)* with $B = \hat{A}$ leads to the required estimates (note that A, $\hat{A}$ are isogenous over k; see for example [La] p. 117). This completes the proof of the present lemma (we ignore the 16 in our favour).

From now on we shall say that the abelian variety A is a product if there are positive integers $e_1, \ldots, e_t$ and simple mutually non-isogenous abelian subvarieties $A_1, \ldots, A_t$ of A such that A is isomorphic to $A_1^{e_1} \times \ldots \times A_t^{e_t}$. The next result extends Lemma 4.1 from simple abelian varieties A to product abelian varieties, and makes the estimate more explicit, at least for $e = 1$ and $N = 8$.

Lemma **6.2.** — *Suppose* A *is a product abelian variety of dimension n, and let* B *be an abelian subvariety of* A^8 *that is isogenous to* A. *Then there is an isogeny from* B *to* A *of degree at most* $c_5(\max\{1, h(A)\})^{n^2\lambda(8n)}$.

Proof. — Assume for the moment only that A is simple. Let e be a positive integer and suppose B is an abelian subvariety of A^{8e} isogenous to A^e. Then by Lemma 4.1 there is an isogeny f from B to A^e with

$$\deg f = N \leqslant (i_e(\mathcal{O}))^{2ne}$$

for $\mathcal{O} = \mathrm{End}\, A$. From the Class Index Lemma we have $N \leqslant |d(\mathcal{O})|^{ne^2}$ and so by Lemma 6.1

(6.3) $$N \leqslant c(\max\{1, h(A)\})^{ne^2\lambda(8n)},$$

where c depends only on n and d.

Now go back to the general situation of the present lemma, and suppose that A is a product $\prod A_i^{e_i}$. Then B is in $\prod A_i^{8e_i}$. Since $A_1, \ldots, A_t$ are simple and mutually non-isogenous, this implies (see for example [MW1] p. 235, 262; all these considerations remain valid over k) that B splits as $\prod B_i$ for B_i in $A_i^{8e_i}$. Clearly B_i is isogenous to $A_i^{e_i}$, so our opening remark and (6.3) provide isogenies f_i from B_i to $A_i^{e_i}$ with

$$\deg f_i = N_i \leqslant c_6(\max\{1, h(A_i)\})^{\lambda_i}$$

and $\lambda_i = n_i e_i^2 \lambda(8n_i)$, where n_i is the dimension of A_i. Using a standard property of Faltings heights (compare (1.2)) we find that

(6.4) $$h(A_i) \leqslant c_7 h$$

for $h = \max\{1, h(A)\}$. So $f = \prod f_i$ is an isogeny from B to A with

$$\deg f = \prod N_i \leqslant c_8 h^{\lambda}$$

and $\lambda = \sum n_i e_i^2 \lambda(8n_i)$. Since $\sum n_i e_i = n$, our monotonicity assumption implies that $\lambda \leqslant n^2 \lambda(8n)$, and this completes the proof.

In a similar way the following result extends Lemma 4.2 from simple abelian varieties A, B to a product situation, and also makes the upper bound more explicit, at least when $B = \hat{A}$.

Lemma **6.3.** — *Suppose* A *is a product abelian variety of dimension* n. *Then there is an isogeny from* $\hat{A}$ *to* A *of degree at most* $c_9(\max\{1, h(A)\})^{n\lambda(8n)}$.

Proof. — As in the proof of the preceding lemma, suppose first that A is simple. Then by Lemma 4.2 with $B = \hat{A}$ there is an isogeny f from $\hat{A}$ to A with

$$\deg f = N \leqslant (c(\mathscr{H}, \mathscr{H}'))^n,$$

where $$\mathscr{H} = \mathrm{Hom}(\hat{A}, A), \quad \mathscr{H}' = \mathrm{Hom}(A, \hat{A}).$$

So by Lemma 6.1 we find that

(6.5) $$N \leqslant c(\max\{1, h(A)\})^{n\lambda(8n)}$$

where c depends only on n and d.

Back in the general situation $A = \prod A_i^{e_i}$, we use (6.5) to derive isogenies f_i from $\hat{A}_i$ to A_i with

$$\deg f_i = N_i \leqslant c_{10}(\max\{1, h(A_i)\})^{\lambda_i}$$

and $\lambda_i = n_i \lambda(8n_i)$. Using (6.4) again we construct this time $f = \prod f_i^{e_i}$ from $\hat{A}$ to A with

$$\deg f = \prod N_i^{e_i} \leqslant c_{11} h^{\lambda}$$

for $$\lambda = \sum n_i e_i \lambda(8n_i) \leqslant n\lambda(8n).$$

This completes the proof.

7. Proof of Theorems

We first treat the rational case. Thus down to equation (7.7) below everything including polarizations is defined over the ground field. We start by recalling the polarized version of our Theorem II proved as the Corollary in [MW4]. Namely, let A, A* be isogenous abelian varieties of dimension n, defined over a number field of degree d, with polarizations of degrees at most δ. Then there is an isogeny f from A to A* with

$$\deg f \leqslant C(\max\{1, h(A)\})^{\mu(n)}, \tag{7.1}$$

where again $\mu(n)$ depends only on n but C depends on δ as well as on n and d.

Our ultimate goal, in Theorem II, is to eliminate the dependence on the polarizations. But first we prove the following intermediate version, independent of polarizations, when A is a product. Again $c_1, c_2, \ldots$ denote constants depending only on n and d.

Lemma 7.1. — *Suppose* A *and* A* *are isogenous abelian varieties of dimension n defined over a number field of degree d, and that* A *is a product. Then there is an isogeny from* A* *to* A *of degree at most* $c_1(\max\{1, h(A)\})^{\kappa_0}$, *with*

$$\kappa_0 = 5n^2\lambda(8n) + 16n\mu(8n).$$

Proof. — Since A and A* are isogenous, so are $Z = Z(A)$ and $Z^* = Z(A^*)$. Because these are principally polarized we can apply (7.1) with $\delta = 1$ to obtain an isogeny p' from Z to Z* with

$$\deg p' = N \leqslant c_2 h^{\mu}$$

where $h = \max\{1, h(A)\}$ and $\mu = \mu(8n)$. So there is an opposite isogeny p from Z* to Z with

$$\deg p = N^{16n-1} \leqslant c_3 h^{16n\mu}. \tag{7.2}$$

By Lemma 6.3 there is an isogeny f from $\hat{A}$ to A with

$$\deg f = M \leqslant c_4 h^{\lambda}$$

and $\lambda = n\lambda(8n)$. Taking the product of f^4 with the identity on A^4 gives an isogeny q from Z to A^8 with

$$\deg q = M^4 \leqslant c_5 h^{4\lambda}. \tag{7.3}$$

Now let i be any embedding of A* into Z* (for example into a direct factor) and consider $B = qpi(A^*)$. This is an abelian subvariety of A^8 and it is isogenous to A because p, q are isogenies, i is an embedding and by hypothesis A* is isogenous to A. So by Lemma 6.2 there is an isogeny r from B to A with

$$\deg r \leqslant c_6 h^{\nu} \tag{7.4}$$

and $\nu = n^2\lambda(8n)$. Now the composition $rqpi$ is an isogeny from A^* to A with degree at most $\deg(rqp)$, which by (7.2), (7.3) and (7.4) is at most $c_7 h^{\kappa_0}$. This completes the proof of Lemma 7.1.

We can now establish the main results of the paper in the rational case. For Theorem I let N be the smallest positive integer for which there exist positive integers $e_1, \ldots, e_t$ and simple mutually non-isogenous abelian subvarieties $A_1, \ldots, A_t$ of A together with an isogeny from A to $A^* = A_1^{e_1} \times \ldots \times A_t^{e_t}$ of degree N. Applying Lemma 7.1 with the abelian varieties switched around, we get an isogeny from A to A^* of degree $N' \leqslant c_8(\max\{1, h(A^*)\})^{\kappa_0}$. Using another standard property (compare (1.1)) of Faltings heights, we see that

$$N' \leqslant c_9(h + \log N)^{\kappa_0}$$

for $h = \max\{1, h(A)\}$. But by minimality $N \leqslant N'$, and we conclude in the usual way that $N \leqslant c_{10} h^{\kappa_0}$. This is nothing else than the assertion of Theorem I (in the rational case).

The proof of Theorem II is even easier. We have just seen from Theorem I that there is an isogeny f from A to some product abelian variety A_0 with

$$\deg f = N \leqslant c_{11} h^{\kappa_0}. \tag{7.5}$$

So by Lemma 7.1 there is an isogeny f^* from A^* to A_0 with

$$\deg f^* \leqslant c_{12}(\max\{1, h(A_0)\})^{\kappa_0}. \tag{7.6}$$

Using (1.1) to estimate $h(A_0)$ in terms of h and $\log N$, and then using (7.5) we get $h(A_0) \leqslant c_{13} h$. Thus (7.6) gives $\deg f^* \leqslant c_{14} h^{\kappa_0}$, and now we can reverse f^* and compose the result with f to obtain the required isogeny of degree at most $c_{15} h^{2n\kappa_0}$.

This completes the proof of Theorems I and II in the rational case; the exponent in both results can be taken as

$$\kappa = 2n\kappa_0 = 10n^3\lambda(8n) + 32n^2\mu(8n), \tag{7.7}$$

where λ and μ are defined in (6.1) and (7.1) respectively.

We now consider the relative case over an arbitrary field K containing k. We need the following result due essentially to Silverberg [S], in which A[3] denotes the set of points of order 3 on an abelian variety A.

Lemma **7.2.** — *a) Suppose* A *is an abelian variety defined over a number field k. Then every abelian subvariety of* A *is defined over the field* $k(A[3])$.

b) Suppose A, A^* *are abelian varieties defined over a number field k. Then every homomorphism from* A *to* A^* *is defined over the field* $k(A[3], A^*[3])$.

Proof. — Part *b)* is a special case of Theorem 2.4 (p. 255) of [S], and then part *a)* follows as in the proof of Lemma 2.2 (p. 414) of [MW2].

Note that if A has dimension n then

$$[k(A[3]) : k] \leqslant 3^{2n}, \tag{7.8}$$

and so this result provides a significant strengthening of Lemmas 2.1 and 2.2 of [MW2].

We now deduce Theorem II for arbitrary K from the rational case. Suppose A, A* are defined over k and isogenous over K. From Lemma 7.2 *b)* it follows that they are isogenous over the field $k_{II} = k(A[3], A^*[3]) \cap K$, which by (7.8) is a number field of degree at most $3^{4n} d$. Now the rational case over k_{II} provides a small isogeny over k_{II} and hence over K. This completes the proof of Theorem II in general, with the same exponent (7.7).

The deduction of Theorem I from the rational case is similar, using the number field $k_I = k(A[3]) \cap K$. We get abelian subvarieties $A_1, \ldots, A_t$ of A, defined over k_I, simple over k_I, and mutually non-isogenous over k_I, together with a small isogeny from A to a product. We claim that $A_1, \ldots, A_t$ are simple and mutually non-isogenous over K.

But suppose for example that B is an abelian subvariety of A_1 defined over K. By Lemma 7.2 *a)* it is defined over $k(A_1[3]) \subseteq k(A[3])$ and so also over k_I. Hence indeed $B = 0$ or A. Similarly suppose for example that f is a homomorphism from A_1 to A_2 defined over K. Then by Lemma 7.2 *b)* it is defined over $k(A_1[3], A_2[3]) \subseteq k(A[3])$ and so also over k_I. Hence indeed $f = 0$.

So the above claim is established, and it follows that we get a factorization over K. This completes the proof of Theorem I in general, also with the exponent (7.7).

Let us now discuss the Corollary. There is an attractive approach to this result, which runs as follows. It is known (see for example [Mu] p. 234) that every abelian variety A is isogenous to a principally polarized abelian variety A*. If we were allowed to apply Theorem II, then we would get a small isogeny f from A to A*, and we could use this to pull back the principal polarization on A*. Unfortunately we are not allowed to apply Theorem II, because the field of definition of A* cannot be controlled, except in terms of some polarization on A!

We obtain a valid proof simply by replacing A* by the dual $\hat{A}$ of A in this argument. If End A is trivial, then it is easy to see that for any isogeny f from A to $\hat{A}$, either f or $-f$ corresponds to a polarization on A. This establishes the Corollary.

It seems to be an interesting problem in itself to generalize the Corollary by removing the hypothesis of trivial endomorphisms. For example, this would provide another more direct route from the polarized isogeny result (7.1) to the unpolarized result of Theorem II. Alternatively one can hope to generalize the Corollary directly using Theorem II, as above. In fact this can be done in a number of cases, and we shall provide details in a later article.

We close the present paper with some remarks about the constants C and κ in our results. As already for [MW2], [MW3] and [MW4], the exponent κ is not only effective but also explicit; however in practice it remains somewhat large. Similarly the constant C can be made explicit in the degree d. In fact it can be supposed independent of d, provided we replace $\max\{1, h(A)\}$ by $\max\{d, h(A)\}$. This follows easily from the analogous modifications of (6.1) and (7.1), which themselves are clear from the inequalities (5.3) and (6.4) of [MW4]. But the effective dependence of C on the dimension n remains an interesting problem.

REFERENCES

[B] D. BERTRAND, *Minimal heights and polarizations on abelian varieties*, preprint M. S. R. I. 06220-87 (June 1987).

[Ca] J. W. S. CASSELS, *Rational quadratic forms*, Academic Press, 1978.

[CR1] C. W. CURTIS and I. REINER, *Representation theory of finite groups and associative algebras*, Interscience Publishers, 1962.

[CR2] C. W. CURTIS and I. REINER, *Methods of representation theory with applications to finite groups and orders*, Vol. I, Wiley-Interscience, 1981.

[F] G. FALTINGS, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.*, **73** (1983), 349-366.

[H] H. HASSE, *Number theory*, Springer, 1980.

[La] S. LANG, *Abelian varieties*, Springer, 1983.

[LOZ] H. W. LENSTRA Jr., F. OORT and Y. ZARHIN, *Abelian subvarieties*, preprint University of Utrecht 842 (March 1994).

[MW1] D. W. MASSER and G. WÜSTHOLZ, Zero estimates on group varieties II, *Invent. Math.*, **80** (1985), 233-267.

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

[MW3] D. W. MASSER and G. WÜSTHOLZ, Isogeny estimates for abelian varieties, and finiteness theorems, *Annals of Math.*, **137** (1993), 459-472.

[MW4] D. W. MASSER and G. WÜSTHOLZ, Endomorphism estimates for abelian varieties, *Math. Z.*, **215** (1994), 641-653.

[Mu] D. MUMFORD, *Abelian varieties*, Oxford, 1974.

[P] R. S. PIERCE, *Associative algebras*, Springer, 1982.

[Re] I. REINER, *Maximal orders*, Academic Press, 1975.

[Ro] L. RONYAI, Zero divisors in quaternion algebras, *J. Algorithms*, **9** (1988), 494-506.

[S] A. SILVERBERG, Fields of definition for homomorphisms of abelian varieties, *J. Pure and Applied Algebra*, **77** (1992), 253-262.

[Z1] Y. ZARHIN, Endomorphisms of abelian varieties and points of finite order in characteristic p, *Mat. Zametki*, **21** (1977), 737-744; *Math. Notes*, **21** (1977), 415-419.

[Z2] Y. ZARHIN, A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction, *Invent. Math.*, **79** (1985), 309-321.

D. W. M.
Mathematisches Institut
Universität Basel
4051 Basel
Switzerland

G. W.
Département für Mathematik
ETH-Zentrum
8092 Zürich
Switzerland

Manuscrit reçu le 26 octobre 1993,
révisé le 4 novembre 1994.