Algebra & Number Theory

Volume 8
2014
No. 5

Polarization estimates for abelian varieties

David Masser and Gisbert Wüstholz

msp

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1045

Polarization estimates for abelian varieties

David Masser and Gisbert Wüstholz

In an earlier paper we showed that an abelian variety over a number field of fixed degree has a polarization whose degree is bounded by a power of its logarithmic Faltings height, provided there are only trivial endomorphisms. Here we greatly relax the endomorphism hypothesis, and we even eliminate it completely when the dimension is at most seven. Our methods ultimately go back to transcendence theory, with the asymmetric geometry of numbers as a new ingredient, together with what we call the Severi–Néron group, a variant of the Néron–Severi group.

1. Introduction

In this paper we address the following question: is the polarization of an abelian variety determined by arithmetical data? More precisely, if A is an abelian variety of fixed dimension defined over a fixed number field, is there necessarily a polarization on A whose degree is bounded in terms of the Faltings height of A?

So formulated, the question has the easy answer, "yes". For a fundamental finiteness result states that, up to isomorphism, there are only finitely many such abelian varieties with a bounded height, and then we can choose a polarization on each of them. However, this argument fails to give any kind of explicit estimate for the degrees of the polarizations.

Taking into account the applications of transcendence theory to abelian varieties in recent years, in particular our papers [Masser and Wüstholz 1993a; 1993b; 1993c; 1994; 1995a; 1995b], one may conjecture that these degrees are bounded by an expression of the form $C \max\{1, h(A)\}^{\pi}$, where $h(A)$ is the absolute logarithmic semistable Faltings height of A (see, for example, [Faltings 1983] or [Bost 1996a]), π depends only on the dimension of A, and C depends only on this dimension together with the degree of the field of definition of A.

The object of the present paper is to establish this conjecture in almost all the cases of interest to algebraists or arithmetic geometers. It was already proved in [Masser and Wüstholz 1995a, Corollary, p. 6] when the endomorphism ring of A is trivial. In general suppose that A is defined over a number field k, and write End A

MSC2010: primary 11G10; secondary 11J95.
Keywords: abelian varieties, estimating polarizations.

for the ring of endomorphisms defined over the algebraic closure $\bar{k}$ of k; this is an order in the algebra $\mathbb{Q} \otimes \mathrm{End}\, A$ over the rational field $\mathbb{Q}$. If A is simple, this algebra is a division algebra whose center is a number field. Our main result can be stated as follows.

Theorem 1.1. *For positive integers n and d there is a constant π depending only on n and a constant C depending only on n and d with the following property. Let A be an abelian variety of dimension n defined over a number field k of degree d. Suppose that A is simple over $\bar{k}$ and that $\mathbb{Q} \otimes \mathrm{End}\, A$ is commutative or its center is totally real. Then A has a polarization over $\bar{k}$ of degree at most $C \max\{1, h(A)\}^{\pi}$.*

In fact the above hypotheses on the endomorphism algebra correspond precisely to the types I, II and III in Albert's famous classification, together with type IV in the commutative case. This remark is already enough to establish the above conjecture for simple abelian varieties in infinitely many dimensions and all abelian varieties, not necessarily simple, in small dimensions. For example, we will deduce the following consequences.

Corollary 1.2. *For a positive squarefree integer n and a positive integer d there is a constant π depending only on n and a constant C depending only on n and d with the following property. Let A be an abelian variety of dimension n defined over a number field k of degree d. Suppose that A is simple over $\bar{k}$. Then A has a polarization over $\bar{k}$ of degree at most $C \max\{1, h(A)\}^{\pi}$.*

Corollary 1.3. *For a positive integer d there is a constant C depending only on d with the following property. Let A be an abelian variety of dimension at most 7 defined over a number field k of degree d. Then A has a polarization over $\bar{k}$ of degree at most $C \max\{1, h(A)\}^{\pi}$, where π is an absolute constant.*

In all of the above results the quantity $C \max\{1, h(A)\}^{\pi}$ can readily be replaced by $C_0 \max\{d, h(A)\}^{\pi}$ with C_0 independent of d; see the remarks in [Masser and Wüstholz 1995a, p. 23]. A more interesting problem is to prove that A has a polarization over k itself of small degree in the above sense, but this seems not to follow from our methods. At any rate we may note that all polarizations of an abelian variety of dimension n defined over a field k of characteristic zero are automatically defined over an extension of k of relative degree at most 3^{16n^4}; see [Masser and Wüstholz 1993a, Lemma 2.3, p. 415].

Our original motivation for estimating polarizations was to extend the isogeny estimates of [Masser and Wüstholz 1993b], for polarized abelian varieties, to unpolarized abelian varieties, simply by providing the latter with explicit polarizations. In fact we solved this isogeny problem in a completely different way in our paper [Masser and Wüstholz 1995a]. Nevertheless we feel that our conjecture has enough independent interest to justify the present paper. And similar problems over finite fields have been studied by Howe [1995].

Actually the proof of our theorem relies heavily on the methods and results of [Masser and Wüstholz 1995a]; in particular we need discriminant estimates and factorization estimates. This paper is based ultimately on the work of [Masser and Wüstholz 1993a], which involves techniques from the theory of transcendental numbers. By contrast, the deduction of our present results from those of [Masser and Wüstholz 1995a] is by purely algebraic methods, together with the geometry of numbers. More precisely, the necessary positive definiteness properties of our polarizations are established using tools from the so-called asymmetric geometry of numbers. For endomorphism algebras of types I, III and IV it suffices to use a theorem of Chalk, but for type II we have to develop what seems to be a new generalization to number fields of a theorem of Blaney. All these results are recorded in Section 2.

In Section 3 we prove some elementary properties of discriminants in quaternion algebras and CM-fields, and in Section 4 we give some analogous results for the cross-discriminants introduced in [Masser and Wüstholz 1995a]. Only instead of considering the full set $\mathrm{Hom}(A, \hat{A})$ of homomorphisms from A into its dual $\hat{A}$, we have to restrict to its subset the Néron–Severi group $\mathrm{NS}(A)$, as well as to a certain complement, which for want of a better name we call the Severi–Néron group $\mathrm{SN}(A)$. Also in this section we record the necessary facts about Albert's classification and the representations of the corresponding endomorphism algebras. Some of this material is borrowed from an article of Shimura [1963].

Then in Sections 5 and 6 we obtain our purely algebraic estimates for polarizations on complex abelian varieties; this enables us to postpone the appeal to [Masser and Wüstholz 1995a] until Section 7, where we establish our theorem and its corollaries.

Of course our results are not quite complete; in fact to prove the full conjecture it remains only to treat simple abelian varieties in the noncommutative case of type IV. We hope to return to this problem in a later paper. For the moment it is perhaps amusing to speculate on whether our conjecture holds with $\pi = 0$; for example, does every abelian variety of dimension 2 defined over $\mathbb{Q}$ have a polarization whose degree is bounded by an absolute constant, say 10^{10}?

And finally we should say something about effectivity. As usual the exponents π in our results are not only effective but also explicitly computable, as already in [Masser and Wüstholz 1993a; 1993b; 1995a]. The effectivity of the coefficients C is known for some time since the work of Bost [1996b]. At any rate the algebraic estimates of our own Sections 2–6 are all completely explicit and it is not until Section 7 that we appeal to [Masser and Wüstholz 1995a].

Some of this work was written up while the first author was visiting Göttingen and Erlangen in 1991 (sic), and he would like to thank S. Patterson and H. Lange for hospitality. Since then the work has been mentioned by Bost in his 1994–95 Séminaire Bourbaki talk [Bost 1996b, p. 126], as well as in [Masser 2006] and [Baker and Wüstholz 2007, p. 164].

Recently É. Gaudron and G. Rémond [2013] sent us a manuscript in which they complete our results. They use the general strategy and methods laid down in our papers [Masser and Wüstholz 1993a; 1993b; 1993c; 1994; 1995a; 1995b], but their details appear to differ from ours. Thus our work is of independent value, not least in our use of the asymmetric geometry of numbers. This topic is relevant to class number problems for quadratic forms over number fields and in our context it brings to the fore some interesting side questions.

2. Asymmetric geometry of numbers

For a positive integer ℓ let Ξ be a lattice in the real Euclidean space $\mathbb{R}^\ell$ with determinant $d(\Xi)$. If $d_1, \dots, d_\ell$ are positive real numbers with $d_1 \cdots d_\ell = d(\Xi)$, Minkowski's theorem in the geometry of numbers (see, for example, [Gruber and Lekkerkerker 1987, Theorem 3, p. 43]) provides nonzero $(\xi_1, \dots, \xi_\ell)$ in Ξ with

$$|\xi_1| \le d_1, \dots, |\xi_\ell| \le d_\ell. \tag{2-1}$$

An asymmetric version of this was established by Chalk; it provides instead $(\xi_1, \dots, \xi_\ell)$ in Ξ with

$$\xi_1 > 0, \dots, \xi_\ell > 0, \quad |\xi_1 \cdots \xi_\ell| \le d(\Xi) \tag{2-2}$$

(see, for example, [Gruber and Lekkerkerker 1987, corollary, p. 598] for a proof of Chalk's original theorem for grids). Note that it is not possible to localize further as in (2-1).

Our first application of these results is as follows. Let K be a totally real number field of degree m, and denote by $\phi_1, \dots, \phi_m$ the different embeddings of K into the real field $\mathbb{R}$. For ξ in K write $N(\xi) = \xi^{\phi_1} \cdots \xi^{\phi_m}$ and $T(\xi) = \xi^{\phi_1} + \cdots + \xi^{\phi_m}$ for the norm and trace, respectively, from K to $\mathbb{Q}$. If $\mathbb{O}$ is an order in K we define in the usual way its discriminant $d(\mathbb{O})$ as the determinant of the matrix with entries $\det T(\xi_i, \xi_j)$, $(1 \le i, j \le m)$, where $\xi_1, \dots, \xi_m$ are elements of any basis of $\mathbb{O}$ over the rational integers $\mathbb{Z}$. Since K is totally real, it is easy to see (for example, as in the proof just below) that $d(\mathbb{O})$ is positive.

Lemma 2.1. *For any nonzero σ in K there exists ξ in $\mathbb{O}$ such that $\sigma\xi$ is totally positive and $|N(\xi)| \le d(\mathbb{O})^{1/2}$.*

Proof. Let $u_1, \dots, u_m$ be the signs of $\sigma^{\phi_1}, \dots, \sigma^{\phi_m}$. As ξ runs over $\mathbb{O}$, the vectors $(u_1\xi^{\phi_1}, \dots, u_m\xi^{\phi_m})$ describe a lattice Ξ in $\mathbb{R}^m$, and it is straightforward to check that its determinant $d(\Xi)$ satisfies $(d(\Xi))^2 = d(\mathbb{O})$. The desired result now follows at once from (2-2). □

Next let n be a positive integer (soon to disappear, so that there is no danger of confusion with $n = \dim A$ in Section 1). Let F be a field (also soon to disappear),

and let Q be a quadratic form on F^n over F. This has a discriminant $d(Q)$ in F defined as the determinant of the matrix with entries $Q(e_i, e_j)$ $(1 \le i, j \le n)$, where Q also denotes the associated bilinear form, and $e_1, \dots, e_n$ are elements of the standard basis of F^n over F.

Suppose for the moment that $K = \mathbb{Q}$ and $F = \mathbb{R}$. If Q is nondegenerate and not negative definite a theorem of Blaney [Gruber and Lekkerkerker 1987, Theorem 4, p. 471] shows how to find small positive values of Q on $\mathbb{Z}^n$. Namely, there exists $(\xi_1, \dots, \xi_n) \in \mathbb{Z}^n$ such that

$$0 < Q(\xi_1, \dots, \xi_n) \le 2^{n-1}|d(Q)|^{1/n}.$$

Our purpose in the rest of this section is to obtain generalizations of this result to arbitrary totally real fields K, with totally positive values of Q on $\mathbb{O}^n$ for some order $\mathbb{O}$ of K. For applications it suffices to restrict ourselves to $n \le 3$ and forms Q defined over K (the latter is not in fact a genuine restriction). In that case the real conjugates $Q^{\phi_1}, \dots, Q^{\phi_m}$ each have a certain signature, and it seems necessary to assume that these are all the same. If this common signature is u, we say that Q has total signature u.

We start with totally positive definite binary forms.

Lemma 2.2. *Let $Q(x, y)$ be a binary quadratic form over K with total signature $(++)$. Then there are ξ, η in $\mathbb{O}$ such that $q = Q(\xi, \eta)$ is totally positive and*

$$N(q) \le 2^m d(\mathbb{O})\,|N(d(Q))|^{1/2}.$$

Proof. Completing the square on each of the positive definite conjugates of Q, we find real numbers a_i, b_i, c_i such that

$$Q^{\phi_i}(x, y) = a_i\big((x - b_i y)^2 + (c_i y)^2\big) \quad (1 \le i \le m). \tag{2-3}$$

In particular

$$d(Q^{\phi_i}) = a_i^2 c_i^2 > 0, \quad a_i > 0 \quad (1 \le i \le m), \tag{2-4}$$

and we can also suppose $c_i > 0$ $(1 \le i \le m)$. Now, as ξ, η run over $\mathbb{O}$, the vectors

$$\big(\xi^{\phi_1} - b_1\eta^{\phi_1}, \eta^{\phi_1}, \dots, \xi^{\phi_m} - b_m\eta^{\phi_m}, \eta^{\phi_m}\big)$$

describe a lattice Ξ in $\mathbb{R}^{2m}$, and it is easy to see that

$$d(\Xi) = \big(d(\mathbb{O})^{1/2}\big)^2 = d(\mathbb{O}).$$

Define C by

$$C^{2m} = c_1 \cdots c_m d(\mathbb{O}); \tag{2-5}$$

then it follows from (2-1) that we can find ξ, η in $\mathbb{O}$, not both zero, with

$$|\xi^{\phi_i} - b_i\eta^{\phi_i}| \le C, \quad |\eta^{\phi_i}| \le C/c_i \quad (1 \le i \le m).$$

So (2-3) gives

$$0 < Q^{\phi_i}\left(\xi^{\phi_i}, \eta^{\phi_i}\right) \le 2C^2 a_i \quad (1 \le i \le m).$$

Hence $q = Q(\xi, \eta)$ is totally positive and

$$N(q) \le 2^m C^{2m} a_1 \cdots a_m = 2^m d(\mathbb{O})\,|N(d(Q))|^{1/2}$$

by (2-4) and (2-5). This completes the proof. □

The analogue for totally indefinite forms seems to lie a little deeper.

Lemma 2.3. *Let $Q(x, y)$ be a binary quadratic form over K with total signature $(+-)$. Then there are ξ, η in $\mathbb{O}$ such that $q = Q(\xi, \eta)$ is totally positive and*

$$N(q) \le 2^m d(\mathbb{O})\,|N(d(Q))|^{1/2}.$$

Proof. This time we factorize each indefinite conjugate as

$$Q^{\phi_i}(x, y) = a_i(x - b_i y)(x - c_i y) \quad (1 \le i \le m)$$

for real a_i, b_i, c_i; in particular

$$d(Q^{\phi_i}) = -\tfrac{1}{4}a_i^2(b_i - c_i)^2 < 0 \quad (1 \le i \le m).$$

Now, as ξ, η run over $\mathbb{O}$, the vectors

$$\left(\xi^{\phi_1} - b_1\eta^{\phi_1}, a_1(\xi^{\phi_1} - c_1\eta^{\phi_1}), \ldots, \xi^{\phi_m} - b_m\eta^{\phi_m}, a_m(\xi^{\phi_m} - c_m\eta^{\phi_m})\right)$$

describe a lattice Ξ in $\mathbb{R}^{2m}$ with

$$d(\Xi) = |a_1 \cdots a_m|\,|b_1 - c_1| \cdots |b_m - c_m|\,d(\mathbb{O}).$$

So Chalk's theorem (2-2) applied to Ξ gives us in a similar way the desired estimate. This completes the proof. □

To extend these results to ternary forms we need a couple of elementary observations. For an order $\mathbb{O}$ in K recall from [Masser and Wüstholz 1995a, p. 8] the class index $i(\mathbb{O}) = i_1(\mathbb{O})$, which is the smallest positive integer I such that every $\mathbb{O}$-module of rank 1 in $\mathbb{O}$ contains a principal $\mathbb{O}$-module of index at most I.

Lemma 2.4. *Given elements ξ, η in $\mathbb{O}$ there are μ, ν in $\mathbb{O}$ with*

$$0 < |N(\nu)| \le i(\mathbb{O})^3$$

such that

$$\nu M \subseteq \mathbb{O}\mu \subseteq M$$

for $M = \mathbb{O}\xi + \mathbb{O}\eta$.

Proof. Of course μ plays the role of a highest common factor of ξ and η. If ξ and η are both zero then the result is trivial with $\mu = 0$, $\nu = 1$. Otherwise M has rank 1 and so there is $\mu \neq 0$ in M with

$$[M : \mathbb{O}\mu] = I \leq i(\mathbb{O}). \tag{2-6}$$

Let L be the $\mathbb{O}$-module of all λ in $\mathbb{O}$ such that $\lambda M \subseteq \mathbb{O}\mu$. Again there is $\nu \neq 0$ in L with

$$[L : \mathbb{O}\nu] = I' \leq i(\mathbb{O}). \tag{2-7}$$

Now $L = L_\xi \cap L_\eta$, where L_ζ is the set of all λ in $\mathbb{O}$ such that $\lambda\zeta$ is in $\mathbb{O}\mu$. So

$$[\mathbb{O} : L] = [\mathbb{O} : L_\xi][L_\xi : L_\xi \cap L_\eta] \leq [\mathbb{O} : L_\xi][\mathbb{O} : L_\eta]. \tag{2-8}$$

Also for any ζ in M we have

$$[\mathbb{O} : L_\zeta] = [\mathbb{O}\zeta : \mathbb{O}\zeta \cap \mathbb{O}\mu] \leq [M : \mathbb{O}\mu] = I,$$

so (2-8) gives $[\mathbb{O} : L] \leq I^2$. Finally this together with (2-6) and (2-7) leads to

$$[\mathbb{O} : \mathbb{O}\nu] = [\mathbb{O} : L][L : \mathbb{O}\nu] \leq I^2 I' \leq i(\mathbb{O})^3,$$

and since the left-hand side is $|N(\nu)|$ (see, for example, [Reiner 1975, Example 3, p. 231] the proof is complete. □

Next we say that a row vector v in $\mathbb{O}^3$ is $\mathbb{O}$-primitive if every nonzero λ in K with λv in $\mathbb{O}^3$ satisfies $|N(\lambda)| \geq 1$.

Lemma 2.5. *Suppose that v_0 in $\mathbb{O}^3$ is $\mathbb{O}$-primitive. Then there are v_1, v_2 in $\mathbb{O}^3$ such that v_0, v_1, v_2 form a matrix V with*

$$0 < |N(\det V)| \leq i(\mathbb{O})^9.$$

Proof. Let $v_0 = (\xi_0, \eta_0, \zeta_0)$. By Lemma 2.4 there are μ, ν in $\mathbb{O}$ with

$$0 < |N(\nu)| \leq i(\mathbb{O})^3 \tag{2-9}$$

such that

$$\nu M \subseteq \mathbb{O}\mu \subseteq M \tag{2-10}$$

for $M = \mathbb{O}\xi_0 + \mathbb{O}\eta_0$. In particular there exist ξ_1, η_1 in $\mathbb{O}$ with $\mu = \eta_1\xi_0 - \xi_1\eta_0$, and we define $v_1 = (\xi_1, \eta_1, 0)$ in $\mathbb{O}^3$. Again by Lemma 2.4 there are μ', ν' in $\mathbb{O}$ with

$$0 < |N(\nu')| \leq i(\mathbb{O})^3 \tag{2-11}$$

such that

$$\nu' M' \subseteq \mathbb{O}\mu' \subseteq M' \tag{2-12}$$

for $M' = \mathbb{O}\mu + \mathbb{O}\zeta_0$. In particular there exist σ, τ in $\mathbb{O}$ with $\mu' = \sigma\mu + \tau\zeta_0$. By (2-10) the numbers $\xi_2 = -\nu\tau\xi_0/\mu$, $\eta_2 = -\nu\tau\eta_0/\mu$ are in $\mathbb{O}$, and so $v_2 = (\xi_2, \eta_2, \sigma\nu)$ is

in $\mathbb{O}^3$. Now we can quickly check that the rows v_0, v_1, v_2 form a matrix V with $\det V = \nu\mu'$; and this is nonzero since $\mu' = 0$ would imply $v_0 = 0$, contradicting primitivity.

It remains to verify the upper bound for $|N(\det V)|$. But (2-10) and (2-12) show that λv_0 is in $\mathbb{O}^3$ for $\lambda = \nu\nu'/\mu'$, so primitivity gives $|N(\mu')| \le |N(\nu\nu')|$. Therefore

$$|N(\det V)| \le \left|N\left(\nu^2\nu'\right)\right| \le i(\mathbb{O})^9$$

by (2-9) and (2-11); and this completes the proof. □

If $\mathbb{O}$ happens to be a maximal order, a more natural proof of Lemma 2.5 might be obtained using the projectivity of torsion-free $\mathbb{O}$-modules. But this does not seem quite straightforward, since our definition of primitivity does not quite imply that $\mathbb{O}^3/\mathbb{O}v_0$ is torsion-free. Further the extension to nonmaximal orders appears to involve exponents of $i(\mathbb{O})$ depending on $m = [K : \mathbb{Q}]$.

In practice we shall estimate $i(\mathbb{O})$ by $d(\mathbb{O})^{1/2}$, as in the class index lemma of [Masser and Wüstholz 1995a, p. 8] for $e = 1$.

At last we can extend the earlier results of this section to ternary forms.

Lemma 2.6. *Let $Q(x, y, z)$ be a ternary quadratic form over K with total signature $(+--)$. Then there are ξ, η, ζ in $\mathbb{O}$ such that $q = Q(\xi, \eta, \zeta)$ is totally positive and*

$$N(q) \le 2^{2m} d(\mathbb{O})^5 |N(d(Q))|^{1/3}.$$

Proof. We follow closely the method in [Gruber and Lekkerkerker 1987, p. 471]. Since K is dense in $\mathbb{R} \otimes K$ it is easy to see that Q takes totally positive values on K^3 and so also on $\mathbb{O}^3$. The norms of these latter values are rational numbers with bounded denominator and so form a discrete set. Thus we can find $v_0 = (\xi_0, \eta_0, \zeta_0)$ in $\mathbb{O}^3$ at which the value $q_0 = Q(\xi_0, \eta_0, \zeta_0)$ is totally positive with minimal norm, say $N_0 = N(q_0)$. Then v_0 must be $\mathbb{O}$-primitive, otherwise we could find a value with strictly smaller norm. We express the variables x, y, z in terms of new variables x', y', z' using the matrix V of Lemma 2.5. So if the new form Q' is defined by $Q'(x', y', z') = Q(x, y, z)$ we now have $q_0 = Q'(1, 0, 0)$. Completing the square on $q_0^{-1}Q'$ gives

$$q_0^{-1}Q'\left(x', y', z'\right) = \left(x' + \alpha y' + \beta z'\right)^2 + Q_1\left(y', z'\right)$$

for α, β in K and a binary form Q_1 over K. Since q_0 is totally positive and Q' has total signature $(+--)$, it follows that Q_1 has total signature $(--)$. Lemma 2.2 applied to $-Q_1$ gives η', ζ' in $\mathbb{O}$ with $q_1 = Q_1(\eta', \zeta')$ totally negative and

$$|N(q_1)| \le 2^m d(\mathbb{O})\, |N(d(Q_1))|^{1/2}.$$

Now

$$d(Q_1) = q_0^{-3} d(Q'), \quad d(Q') = (\det V)^2 d(Q)$$

and so the estimate of Lemma 2.5 and the class index lemma lead to

$$|N(q_1)| \le 2^m N_0^{-3/2} d(\mathbb{O})^{11/2} |N(d(Q_1))|^{1/2}. \tag{2-13}$$

Next define a third form over K by

$$Q''(x'', y'') = q_0^{-1} Q'(x'', \eta' y'', \zeta' y'') = (x'' + \gamma y'')^2 + q_1 (y'')^2$$

for some γ in K. This has total signature $(+\,-)$. So Lemma 2.3 gives ξ'', η'' in $\mathbb{O}$ with $q'' = Q''(\xi'', \eta'')$ totally positive and $N(q'') \le 2^m d(\mathbb{O})\, |N(d(Q''))|^{1/2}$. Using the estimate (2-13) for $d(Q'') = q_1$ we find that

$$N(q'') \le 2^{3m/2} N_0^{-3/4} d(\mathbb{O})^{15/4} |N(d(Q_1))|^{1/4}. \tag{2-14}$$

Finally $q = Q'(\xi'', \eta'\eta'', \zeta'\eta'') = q_0 q''$ is a totally positive value of Q' on $\mathbb{O}^3$ and so a totally positive value of Q on $\mathbb{O}^3$. Therefore minimality implies $N_0 \le N(q)$, or $N(q'') \ge 1$. Now (2-14) leads at once to the required upper bound for N_0, and this completes the proof. □

Lemmas 2.2, 2.3, and 2.6 above are all partial generalizations of Blaney's theorem from the rationals to totally real number fields. There is no difficulty in extending the induction argument, as in [Gruber and Lekkerkerker 1987, p. 471], to any number of variables, provided one assumes that Q has a total signature which is not negative definite. But it does not seem straightforward to prove the analogous results under the weaker and more natural hypothesis that no conjugate of Q is negative definite.

3. Quaternion algebras and CM-fields

As in the preceding section, let K be a totally real number field of degree m. Let D be a quaternion algebra over K; that is, a noncommutative algebra over K of dimension 4 with center K. For a finitely generated additive subgroup Γ of D of rank r we define the discriminant $d_1(\Gamma)$ as the determinant of the matrix with entries $T_1(\gamma_i \gamma_j)$ $(1 \le i, j \le r)$, where $\gamma_1, \ldots, \gamma_r$ are elements of any $\mathbb{Z}$-basis for Γ, and T_1 denotes the trace from D to $\mathbb{Q}$ obtained for example through left (or right) regular representations. We also have for all δ in D

$$T_1(\delta) = 2T(\operatorname{tr} \delta), \tag{3-1}$$

where as before T is the trace from K to $\mathbb{Q}$ and now tr is the reduced trace from D to K; see, for example, [Reiner 1975, Example 5, p. 7 and Equation (9.7), p. 116] .

There is a canonical involution ρ_0 on D defined by

$$\rho_0(\delta) = (\operatorname{tr} \delta) - \delta \tag{3-2}$$

for all δ in D. Its fixed space, consisting of all δ with $\rho_0(\delta) = \delta$, is just K; while its antifixed space, consisting of all δ with $\rho_0(\delta) = -\delta$, is a K-vector space E of dimension 3. So $D = K \oplus E$.

The following result specifies the ternary quadratic form to which Lemma 2.6 will eventually be applied. Denote the reduced norm from D to K by

$$\mathrm{nm}\,\delta = \delta\rho_0(\delta) = \rho_0(\delta)\delta,$$

and let N as before be the norm from K to $\mathbb{Q}$.

Lemma 3.1. *If α, β, γ are elements of E linearly independent over K, the quadratic form*

$$Q(x, y, z) = -(x\alpha + y\beta + z\gamma)^2 = \mathrm{nm}(x\alpha + y\beta + z\gamma)$$

satisfies

$$N(d(Q)) = (-1)^m d_1(M) d_1(\mathbb{O})^{-3} \tag{3-3}$$

for any order $\mathbb{O}$ in K, where $M = \mathbb{O}\alpha \oplus \mathbb{O}\beta \oplus \mathbb{O}\gamma$.

Proof. If $\xi_1, \ldots, \xi_m$ are elements of a $\mathbb{Z}$-basis for $\mathbb{O}$, then for any λ in K the matrix with entries $T_1(\xi_i \xi_j \lambda)$ $(1 \le i, j \le m)$ has determinant $d_1(\mathbb{O}) N(\lambda)$. We can find a K-basis of E consisting of elements $\alpha_0, \beta_0, \gamma_0$ satisfying the standard quaternion relations

$$\alpha_0^2 = \xi, \quad \beta_0^2 = \eta, \quad \gamma_0 = \alpha_0\beta_0 = -\beta_0\alpha_0$$

for ξ, η in K, and now (3-3) follows after a short calculation with $\alpha_0, \beta_0, \gamma_0$ in place of α, β, γ; in fact both sides have the value $N(\xi\eta)^2$.

Next let α, β, γ in E be such that $M = \mathbb{O}\alpha \oplus \mathbb{O}\beta \oplus \mathbb{O}\gamma$ is a submodule of $M_0 = \mathbb{O}\alpha_0 \oplus \mathbb{O}\beta_0 \oplus \mathbb{O}\gamma_0$, so that α, β, γ are related to $\alpha_0, \beta_0, \gamma_0$ by means of a nonsingular matrix V over $\mathbb{O}$. If we can check that

$$|N(\det V)| = [M_0 : M], \tag{3-4}$$

then both sides of (3-3) change by the square of this quantity on replacing M_0 by M, so (3-3) follows for α, β, γ.

Now (3-4) should be in the literature, but we could not find an exact reference. It can be verified *ad hoc* by picking a $\mathbb{Z}$-basis of $\mathbb{O}$ and for each λ in K writing V_λ for the matrix in the corresponding right regular representation; then if V has entries λ, the index $[M_0 : M]$ is the absolute value of the determinant of the matrix with blocks V_λ. By [Reiner 1975, Example 3, p. 7] this determinant is just $N(\det V)$. See also [Reiner 1975, Example 3, p. 231] for another approach. Or one can compare the maximal exterior powers of M and M_0; these have the shape $\mathcal{P}(\det V)$, $\mathcal{P}$ for an $\mathbb{O}$-module $\mathcal{P}$ of rank 1.

Hence (3-3) is established for any such α, β, γ. Finally the general case can be reduced to this case simply by multiplying by a suitable positive integer; and the proof of the present lemma is thereby complete. □

Notice in this lemma that $d_1(\mathbb{O})$ is not quite the same as the $d(\mathbb{O})$ in Section 2; in fact

$$d_1(\mathbb{O}) = 4^m d(\mathbb{O}) \tag{3-5}$$

due to the differing traces.

Next let K_1 be a CM-field over K; that is, a totally imaginary quadratic extension of K. For a finitely generated additive subgroup Γ of K_1 we define the discriminant $d_1(\Gamma)$ as above using the trace T_1 from K_1 to $\mathbb{Q}$. The analogue of (3-1) is

$$T_1(\delta) = T(\operatorname{tr}\delta), \tag{3-6}$$

where T is the trace from K to $\mathbb{Q}$ and tr is the (reduced) trace from K_1 to K. There is a canonical involution ρ_0 on K_1, which we can identify with complex conjugation, and (3-2) continues to hold. We define as before E as the antifixed space, so that $K_1 = K \oplus E$.

Lemma 3.2. *Let $\mathbb{O}_1$ be an order of either D or K_1. Then*:

(a) $|d_1(K \cap \mathbb{O}_1)| \le 2^{4m} |d_1(\mathbb{O}_1)|$.

(b) $|d_1(E \cap \mathbb{O}_1)| \le 2^{4m} |d_1(\mathbb{O}_1)|$.

Proof. Suppose first that $\mathbb{O}_1$ is a maximal order. If $\mathbb{O}_K$ is the ring of integers of K then $\mathbb{O}_K\mathbb{O}_1$ contains $\mathbb{O}_1$ and so must be $\mathbb{O}_1$. In particular $\mathbb{O}_1$ is an $\mathbb{O}_K$-order containing $\mathbb{O}_K$. So [Reiner 1975, Theorem 10.1, p. 125] shows that $\operatorname{tr}\delta$ is in $\mathbb{O}_K$ for all δ in $\mathbb{O}_1$. In particular $\operatorname{tr}\delta$ is in $\mathbb{O}_1$, and now the identity $2\delta = \operatorname{tr}\delta + (2\delta - \operatorname{tr}\delta)$ leads to

$$2\mathbb{O}_1 \subseteq (K \cap \mathbb{O}_1) \oplus (E \cap \mathbb{O}_1) \subseteq \mathbb{O}_1.$$

Since the summands are perpendicular with respect to the reduced trace, and therefore by (3-1), (3-6) also with respect to T_1, taking discriminants gives

$$2^{4m} |d_1(\mathbb{O}_1)| \ge |d_1(K \cap \mathbb{O}_1)|\, |d_1(E \cap \mathbb{O}_1)| \ge |d_1(\mathbb{O}_1)|.$$

Since all these discriminants are nonzero rational integers, (a) and (b) follow when $\mathbb{O}_1$ is maximal.

In general there is a maximal order $\mathbb{O}_m$ containing $\mathbb{O}_1$, and

$$d_1(\mathbb{O}_1) = [\mathbb{O}_m : \mathbb{O}_1]^2 d_1(\mathbb{O}_m),$$

$$d_1(K \cap \mathbb{O}_1) = [K \cap \mathbb{O}_m : K \cap \mathbb{O}_1]^2 d_1(K \cap \mathbb{O}_m).$$

But the second index above does not exceed the first index, so (a) follows in general; and (b) is established similarly. This completes the proof. □

4. Polarizations and representations

Let A be an abelian variety defined over the field $\mathbb{C}$ of complex numbers. Analytically A is isomorphic to the quotient of the tangent space Lie A at the origin by the period group Per A defined as the kernel of the exponential map from Lie A to A.

We write $\hat{A}$ for the dual abelian variety of A. Then Lie $\hat{A}$ can be identified with the space of all $\mathbb{C}$-antilinear maps from Lie A to $\mathbb{C}$, and Per $\hat{A}$ with the subgroup of all such maps whose imaginary parts are integer-valued on Per A (see [Lange and Birkenhake 1992, pp. 35, 73] or [Mumford 1974, p. 86]). Now a homomorphism f from A to $\hat{A}$ takes an element z of Lie A to an element of Lie $\hat{A}$ which itself takes (antilinearly) an element w of Lie A into an element $R(z, w)$ of $\mathbb{C}$. In this way the group $\mathcal{H} = \mathrm{Hom}(A, \hat{A})$ of all homomorphisms f from A to $\hat{A}$ is identified with the group of sesquilinear forms $R = R(z, w)$ (linear in z and antilinear in w) on Lie $A \times$ Lie A whose imaginary parts are integer-valued on Per $A \times$ Per A. The dual map $\hat{f}$ (corresponding to $\overline{R(w, z)}$) is also in $\mathcal{H}$, and we can identify the Néron–Severi group $\mathcal{N} = \mathrm{NS}(A)$ with the subgroup of all such f satisfying $\hat{f} = f$. These correspond to Hermitian R. We shall also be interested in the complementary group $\mathcal{S} = \mathrm{SN}(A)$ of all f with $\hat{f} = -f$. For example, the sum of $\mathrm{NS}(A)$ and $\mathrm{SN}(A)$ is direct, lying between $2\mathcal{H}$ and $\mathcal{H}$.

Interchanging A and $\hat{A}$, we obtain in a similar way the groups

$$\mathcal{H}' = \mathrm{Hom}(\hat{A}, A), \quad \mathcal{N}' = \mathrm{NS}(\hat{A}), \quad \mathcal{S}' = \mathrm{SN}(\hat{A}).$$

For f in $\mathcal{H}$ and f' in $\mathcal{H}'$ we denote by $f'f$ the composition in the ring End A of endomorphisms of A.

Next let Γ, Γ' be additive subgroups of $\mathcal{H}, \mathcal{H}'$, respectively, with the same rank, say r. We define the cross-discriminant $c(\Gamma', \Gamma)$, as in [Masser and Wüstholz 1995a, p. 15], as the square of the determinant of the matrix with entries $T_1(\gamma_i' \gamma_j)$ $(1 \le i, j \le r)$, where $\gamma_1, \dots, \gamma_r$ and $\gamma_1', \dots, \gamma_r'$ are elements of $\mathbb{Z}$-bases of Γ, Γ', respectively, and T_1 is the trace from $\mathbb{Q} \otimes \mathrm{End}\, A$ to $\mathbb{Q}$ obtained through regular representations.

From now on (except briefly in Section 7) we shall assume that A is absolutely simple. The next lemma can be regarded as an analogue of Lemma 3.2.

Lemma 4.1. *Suppose that* End A *has* $\mathbb{Z}$*-rank* ℓ. *Then*:

(a) $1 \le c(\mathcal{N}', \mathcal{N}) \le 2^{4\ell} c(\mathcal{H}', \mathcal{H})$.

(b) $1 \le c(\mathcal{S}', \mathcal{S}) \le 2^{4\ell} c(\mathcal{H}', \mathcal{H})$.

Proof. Since $\mathcal{H}$ contains surjective homomorphisms (for example coming from polarizations as in the discussion below), it is easy to see that both $\mathcal{H}$ and $\mathcal{H}'$ have $\mathbb{Z}$-rank ℓ. Further

$$2\mathcal{H} \subseteq \mathcal{N} \oplus \mathcal{S} \subseteq \mathcal{H}, \quad 2\mathcal{H}' \subseteq \mathcal{N}' \oplus \mathcal{S}' \subseteq \mathcal{H}',$$

and taking cross-discriminants gives

$$2^{4\ell} c(\mathcal{H}', \mathcal{H}) \geq c(\mathcal{N}' \oplus \mathcal{S}', \mathcal{N} \oplus \mathcal{S}) = c(\mathcal{N}', \mathcal{N}) c(\mathcal{S}', \mathcal{S}) \geq c(\mathcal{H}', \mathcal{H}) \tag{4-1}$$

provided we check that $\mathcal{N}$ and $\mathcal{S}'$ (as well as $\mathcal{N}'$ and $\mathcal{S}$) are perpendicular with respect to T_1. But this trace is proportional (see [Masser and Wüstholz 1995a, Equation (4.1), p. 14]) to the rational representation trace coming from homology, which is itself proportional to the real part of the analytic representation trace Tr (see, for example, [Lange and Birkenhake 1992, Proposition 2.3, p. 10]). Now pick basis elements of Lie A and then basis elements of Lie $\hat{A}$ dual with respect to the standard pairing. Then f in $\mathcal{N}$ corresponds to a Hermitian matrix F, and f' in $\mathcal{S}'$ corresponds to an antihermitian matrix F'. With the transposes F^t, F'^t we have

$$\operatorname{Tr}(F'F) = \operatorname{Tr}(FF') = \operatorname{Tr}(F'^t F^t) = -\operatorname{Tr}(\bar{F}'\bar{F})$$

and so the real part of $\operatorname{Tr}(F'F)$ is zero. Hence $\mathcal{N}, \mathcal{S}'$ are indeed perpendicular; and similarly for $\mathcal{N}', \mathcal{S}$. Now [Masser and Wüstholz 1995a, Lemma 5.1(b), p. 17] and the nonvanishing of discriminants implies that $c(\mathcal{H}', \mathcal{H}) \neq 0$. Since all the cross-discriminants in (4-1) are rational integers, the inequalities of the present lemma follow at once, and this completes the proof. □

The next result generalizes [Masser and Wüstholz 1995a, Lemma 4.2, p. 16], at least when $B = \hat{A}$. Note that through composition $\mathcal{H}$ and $\mathcal{H}'$ have natural structures of right and left modules, respectively, over $\operatorname{End} A$. We write $\deg \delta$ for the degree of δ in $\operatorname{End} A$ when it is an isogeny. As in Section 1 let n be the dimension of A.

Lemma 4.2. *Let $\mathbb{O}$ in $\operatorname{End} A$ be an order of a division subalgebra of $\mathbb{Q} \otimes \operatorname{End} A$. Suppose that Γ in $\mathcal{H}$ is a right $\mathbb{O}$-module of rank 1 and that Γ' in $\mathcal{H}'$ is a left $\mathbb{O}$-module of rank 1. Suppose further that $c(\Gamma', \Gamma) \neq 0$ and $f'f$ is in $\mathbb{O}$ for every f in Γ and f' in Γ'. Then there are f in Γ and f' in Γ' such that $f'f$ is an isogeny with*

$$\deg f'f \leq c(\Gamma', \Gamma)^n.$$

Proof. There exists f in Γ with

$$[\Gamma : f\mathbb{O}] = I' \leq i'(\mathbb{O})$$

the right class index of $\mathbb{O}$ (see [ibid., p. 13]). And there exists f' in Γ' with

$$[\Gamma' : \mathbb{O}f'] = I \leq i(\mathbb{O})$$

the left class index. The class index lemma of [ibid., p. 8], together with [ibid., Equation (3.11), p. 14], provides estimates for these class indices in terms of the discriminant of $\mathbb{O}$, which divides the discriminant $d_1(\mathbb{O})$ defined using the present trace T_1 (compare (3-5) above). We get

$$c(\mathbb{O}f', f\mathbb{O}) = I^2 I'^2 c(\Gamma', \Gamma) \leq d_1(\mathbb{O})^2 c(\Gamma', \Gamma). \tag{4-2}$$

On the other hand the left side is the square of the determinant of the matrix with entries $T_1(\xi_i \delta \xi_j)$ $(1 \le i, j \le r)$ for $\delta = f'f$ and elements $\xi_1, \dots, \xi_r$ of a $\mathbb{Z}$-basis of $\mathcal{O}$. Using the left (or right) regular representation of δ in $\mathcal{O}$, we find (much as in the proof of Lemma 3.1) that this determinant is $N d_1(\mathcal{O})$, where N is the norm of δ from $\mathbb{Q} \otimes \mathcal{O}$ to $\mathbb{Q}$. In particular $N \neq 0$ so δ is an isogeny. Finally comparison of norms (see [Masser and Wüstholz 1995a, Equation (4.2), p. 14]) yields

$$N^{2n} = (\deg \delta)^r \ge \deg \delta,$$

and the present lemma follows from (4-2) after cancellation. This completes the proof. □

The ultimate goal of this paper is to obtain information about the polarizations on A. These may be identified with the subset $\operatorname{Pol} A$ of $\operatorname{NS}(A)$ corresponding to positive definite Hermitian forms. Recall that every such polarization f gives rise to its Rosati involution ρ on $\mathbb{Q} \otimes \operatorname{End} A$ by the equation

$$\rho(\delta) = f^{-1} \hat{\delta} f. \tag{4-3}$$

It is well known (see, for example, [Lange and Birkenhake 1992, Theorem 1.8, p. 120] or [Mumford 1974, Theorem 1, p. 192]) that ρ is a positive involution in the sense that $T_1(\delta \rho(\delta)) > 0$ for all nonzero δ in $\mathbb{Q} \otimes \operatorname{End} A$.

The existence of ρ provides a quick method for calculating $\operatorname{NS}(A)$. For multiplication on the left by f^{-1} gives a (noncanonical) identification of $\mathbb{Q} \otimes \operatorname{Hom}(A, \hat{A})$ with $\mathbb{Q} \otimes \operatorname{End} A$, and $\mathbb{Q} \otimes \operatorname{NS}(A)$ corresponds to the fixed space of ρ (see [Lange and Birkenhake 1992, Proposition 2.1(a), p. 122] or [Mumford 1974, p. 190]). Similarly $\operatorname{SN}(A)$ corresponds to the antifixed space. Further, multiplication on the right by f gives an identification of $\mathbb{Q} \otimes \operatorname{Hom}(\hat{A}, A)$ with $\mathbb{Q} \otimes \operatorname{End} A$; and now it is $\mathbb{Q} \otimes \operatorname{NS}(\hat{A})$ and $\mathbb{Q} \otimes \operatorname{SN}(\hat{A})$ that correspond to the fixed and antifixed spaces, respectively, of ρ.

Recall that A is absolutely simple. Then $D = \mathbb{Q} \otimes \operatorname{End} A$ is a division algebra, and we have the following fundamental classification due to Albert (see, for example, the summaries in [Lange and Birkenhake 1992], [Mumford 1974], [Shimura 1963] or the original papers [Albert 1934a; 1935a; 1934b; 1935b]).

Type I: D is a totally real number field.

Type II: D is a totally indefinite quaternion algebra over a totally real number field.

Type III: D is a totally definite quaternion algebra over a totally real number field.

Type IV: D is a division algebra, of dimension e^2 say, over its center, which is a CM-field.

For each type the underlying totally real number field will be denoted by K, and its degree by m. Let $\phi_1, \ldots, \phi_m$ be the different real embeddings of K as in Section 2. For a field F we denote by $\mathcal{M}_e(F)$ the ring of square matrices of order e over F, and we write $\boldsymbol{U}$ for the subring of $\mathcal{M}_2(\mathbb{C})$ consisting of all $\left(\begin{smallmatrix} x & y \\ -\bar{y} & \bar{x} \end{smallmatrix}\right)$. The operation of complex conjugate transposition defines an involution * on $\mathcal{M}_e(\mathbb{R})$, $\mathcal{M}_e(\mathbb{C})$ and $\boldsymbol{U}$, which we extend to m-fold products in the obvious way. We need the following isomorphisms.

Lemma 4.3. *Fix f in* Pol A *with Rosati involution ρ. Then the above real embeddings induce an isomorphism $\phi = (\phi_1, \ldots, \phi_m)$ from $\mathbb{R} \otimes D$ to one of the following rings* (*corresponding to the above types*):

(I) $\mathbb{R}^m = \mathcal{M}_1(\mathbb{R})^m$,

(II) $\mathcal{M}_2(\mathbb{R})^m$,

(III) $\boldsymbol{U}^m$,

(IV) $\mathcal{M}_e(\mathbb{C})^m$.

Further we have

$$\phi(\rho(\delta)) = \phi(\delta)^* \tag{4-4}$$

for every δ in $\mathbb{R} \otimes D$; and for every σ in K, the matrix $\phi_i(\sigma)$ is the identity multiplied by σ^{ϕ_i} $(1 \le i \le m)$.

Proof. All except the last clause is contained in the discussions in [Lange and Birkenhake 1992, pp. 133–141], [Mumford 1974, pp. 201, 202] or [Shimura 1963, pp. 150–153, 155]. As for $\phi_1(\sigma), \ldots, \phi_m(\sigma)$, they must be in the centers of the appropriate rings and therefore multiples of the identity matrix by some scalars. Further these scalars must have the form $\sigma^{\phi_1'}, \ldots, \sigma^{\phi_m'}$ for $\phi_1', \ldots, \phi_m'$ chosen from $\phi_1, \ldots, \phi_m$. But since ϕ is surjective, $\phi_1', \ldots, \phi_m'$ must be all different, and after a permutation we can assume them to be $\phi_1, \ldots, \phi_m$. This completes the proof. □

We next extend ϕ to an analytic representation of $\mathbb{R} \otimes D$ on the tangent space Lie A. Let $\bar{\phi}_1, \ldots, \bar{\phi}_m$ be the complex conjugates of the coordinates of ϕ. For matrices X in $\mathcal{M}_e(\mathbb{C})$ with entries x_{ij} $(1 \le i, j \le e)$, and Y in $\mathcal{M}_h(\mathbb{C})$, define the Kronecker product $X \otimes Y$ in $\mathcal{M}_{eh}(\mathbb{C})$ as in [Shimura 1963, p. 156] or [Lange and Birkenhake 1992, p. 249] to consist of blocks $x_{ij}Y$ $(1 \le i, j \le e)$. Also for matrices $X_1, \ldots, X_k$ define $\operatorname{diag}(X_1, \ldots, X_k)$ as in this last reference, with blocks $X_1, \ldots, X_k$ "down the main diagonal". Finally write $I(e)$ for the identity in $\mathcal{M}_e(\mathbb{C})$.

Lemma 4.4. *Fix f in* Pol A. *There is a basis of* Lie A *such that the corresponding analytic representation Φ sends δ in $\mathbb{R} \otimes D$ to $\Phi(\delta) = \operatorname{diag}(\Phi_1(\delta), \ldots, \Phi_m(\delta))$, with*

(I) $\Phi_i(\delta) = \phi_i(\delta) \otimes I(n/m) \quad (1 \le i \le m)$,

(II) $\Phi_i(\delta) = \phi_i(\delta) \otimes I(n/2m) \quad (1 \le i \le m)$,

(III) $\Phi_i(\delta) = \phi_i(\delta) \otimes I(n/2m) \quad (1 \le i \le m)$,

(IV) $\Phi_i(\delta) = \operatorname{diag}\big(\phi_i(\delta) \otimes I(r_i), \bar{\phi}_i(\delta) \otimes I(s_i)\big) \quad (1 \le i \le m)$

for nonnegative integers r_i, s_i *with* $r_i + s_i = n/em$ $(1 \le i \le m)$.

Proof. See [Shimura 1963, pp. 156, 157]; of course if $r_i = 0$ or $s_i = 0$ then the corresponding block in case (IV) should be omitted. □

The above result leads to the following for the Riemann form $R(z, w)$ associated with the polarization f, where now $z = (z_1, \dots, z_n)^t$, $w = (w_1, \dots, w_n)^t$ are column vectors of $\mathbb{C}^n$ identified with Lie A by means of the above basis.

Lemma 4.5. *Fix* f *in* Pol A; *then with the basis of* Lie A *constructed above, the Riemann form* $R(z, w)$ *associated with* f *has the shape* $z^t F \bar{w}$ *for*

$$F = \operatorname{diag}(F_1, \dots, F_m)$$

with

(I) F_i *of order* $n/m \quad (1 \le i \le m)$,

(II) $F_i = I(2) \otimes F_i'$ *for* F_i' *of order* $n/2m \quad (1 \le i \le m)$,

(III) $F_i = I(2) \otimes F_i'$ *for* F_i' *of order* $n/2m \quad (1 \le i \le m)$,

(IV) $F_i = \operatorname{diag}(I(e) \otimes G_i, I(e) \otimes H_i)$ *for* G_i, H_i *of orders* r_i, s_i, *respectively* $(1 \le i \le m)$.

Proof. The equation (4-3) of ρ leads to

$$R(z, \Phi(\delta)w) = R(\Phi(\rho(\delta))z, w)$$

for every δ in End A. With $r(z, w) = z^t F \bar{w}$ it follows from (4-4) that $F\bar{\Phi}(\delta) = \bar{\Phi}(\delta)F$ for every such δ, and so also for every δ in $\mathbb{R} \otimes D$. Therefore F commutes with every element of $\bar{\Phi}(\mathbb{R} \otimes D) = \Phi(\mathbb{R} \otimes D)$. The required forms are now easy to work out; see, for example, [Shimura 1963, Formulae (32), (33), pp. 161, 162]. This completes the proof. □

5. Preliminary estimates (i)

In this section we establish preliminary estimates for polarizations on simple abelian varieties with endomorphism algebras of types I, III and the commutative case $e = 1$ of type IV. These cases are especially easy to handle because there is only one positive involution on $D = \mathbb{Q} \otimes \text{End } A$ (see [Lange and Birkenhake 1992, Theorem 5.3, p. 135 and Theorem 5.6, p. 139] or [Mumford 1974, Theorem 2, p. 201]). For type I it is the identity; for type III it is the canonical involution of Section 3; and for type IV it induces complex conjugation on the center, so in the commutative case it is also the canonical involution considered in Section 3.

Therefore the totally real number field K is always the fixed space. For the rest of this section we assume that A is simple corresponding to one of the above cases. We write

$$\mathbb{O}_1 = \operatorname{End} A, \quad \mathbb{O} = K \cap \mathbb{O}_1. \tag{5-1}$$

Lemma 5.1. *Suppose that f is in* Pol A *and ζ is totally positive in $\mathbb{O}$. Then $f\zeta$ is in* Pol A.

Proof. Shimura [1963, Proposition 21, p. 185] gives a short elegant proof of this based on Siegel's theorem that ζ is a sum of squares in K. The following demonstration is more elementary.

By Lemma 4.5 the polarization f corresponds to the form $z^t F \bar{w}$ with

$$F = \operatorname{diag}(F_1, \ldots, F_m)$$

(with respect to a suitable basis). So $f\zeta$ corresponds to the form $z^t F_\zeta \bar{w}$ with $F_\zeta = \Phi(\zeta)^t F$. Now it follows easily from Lemmas 4.3 and 4.4 that

$$\Phi(\zeta)^t = \Phi(\zeta) = \operatorname{diag}(\zeta^{\phi_1} I, \ldots, \zeta^{\phi_m} I)$$

for $I = I(n/m)$, and so

$$F_\zeta = \operatorname{diag}(\zeta^{\phi_1} F_1, \ldots, \zeta^{\phi_m} F_m).$$

Since f is a polarization, F is positive definite Hermitian. Therefore $F_1, \ldots, F_m$ are positive definite Hermitian. Since ζ is totally positive, it follows that $\zeta^{\phi_1} F_1, \ldots, \zeta^{\phi_m} F_m$ are also positive definite Hermitian. Hence F_ζ is positive definite Hermitian, and so $f\zeta$ is indeed a polarization. This completes the proof, which works even for the noncommutative case of type IV. □

Lemma 5.2. *The group $\mathcal{N} = \mathrm{NS}(A)$ is a right $\mathbb{O}$-module of rank* 1; *the group $\mathcal{N}' = \mathrm{NS}(\hat{A})$ is a left $\mathbb{O}$-module of rank* 1; *and $f'f$ is in $\mathbb{O}$ for every f in $\mathcal{N}$ and f' in $\mathcal{N}'$.*

Proof. The claims for $\mathcal{N}$ can be checked by noncanonically identifying $\mathbb{Q} \otimes \mathcal{H}$ with $D = \mathbb{Q} \otimes \mathbb{O}_1$ as described in Section 4; this identification respects the right D-module structure. For type I every Rosati involution is the identity; so $\mathcal{N} = \mathcal{H}$, $\mathcal{S} = \{0\}$ and everything is clear. For type III every Rosati involution ρ is canonical, so $\mathcal{H}$, $\mathcal{N}$, $\mathcal{S}$ have $\mathbb{Z}$-ranks $4m$, m, $3m$, respectively. So the asserted $\mathbb{O}$-module structure of $\mathcal{N}$ is obvious because ρ fixes $\mathbb{O}$. For the commutative case of type IV, every Rosati involution is again canonical, so $\mathcal{H}$, $\mathcal{N}$, $\mathcal{S}$ have $\mathbb{Z}$-ranks $2m$, m, m, respectively, and again ρ fixes $\mathbb{O}$.

The claims about $\mathcal{N}'$ can be verified similarly by identifying $\mathbb{Q} \otimes \mathcal{H}'$ with D. Finally let f be in $\mathcal{N}$ and f' in $\mathcal{N}'$. It is easy to see that $\mathbb{Q} \otimes \mathcal{N}$ is generated by polarizations. So in proving that $\delta = f'f$ is in $\mathbb{O}$ we may assume that f is a

polarization. Now using $\hat{f} = f$ and a similar equation for f' we find at once that $f^{-1}\hat{\delta} f = \delta$, so δ is fixed by the Rosati involution. So it lies in K and therefore in $\mathbb{O}$ as desired. This completes the proof. □

We can now give our first preliminary estimate for polarizations. We write $\deg f$ for the degree of f in $\mathcal{H} = \mathrm{Hom}(A, \hat{A})$ when it is an isogeny (that is, when $f \neq 0$).

Proposition 5.3. *Suppose that A is simple and its endomorphism algebra is either commutative or a totally definite quaternion algebra over a totally real number field. Then A has a polarization of degree at most $2^{18mn} c(\mathcal{H}', \mathcal{H})^n |d_1(\mathbb{O}_1)|^n$.*

Proof. From Lemma 4.1(a) we have $c(\mathcal{N}', \mathcal{N}) \neq 0$. Now Lemma 5.2 above allows us to apply Lemma 4.2 with $\Gamma = \mathcal{N}, \Gamma' = \mathcal{N}'$ to find an isogeny $\tilde{f}$ in $\mathcal{N}$ with $\deg \tilde{f} \leq c(\mathcal{N}', \mathcal{N})^n$. Again using Lemma 4.1(a) and the fact that $\ell \leq 4m$ in our situation, we get

$$\deg \tilde{f} \leq 2^{16mn} c(\mathcal{H}', \mathcal{H})^n. \tag{5-2}$$

Now there is certainly some polarization f; so we deduce $\tilde{f} = f\sigma$ for some nonzero σ in K. By Lemma 2.1 there is a ξ in $\mathbb{O}$ with $\xi\sigma$ totally positive and $|N(\xi)| \leq d(\mathbb{O})^{1/2}$. Also Lemma 3.2(a) together with (3-5) gives $d(\mathbb{O}) \leq 2^{2m} |d_1(\mathbb{O}_1)|$, and so we get

$$\deg \xi = |N(\xi)|^{2n/m} \leq N(\xi)^{2n} \leq 2^{2mn} |d_1(\mathbb{O}_1)|^n. \tag{5-3}$$

It is clear from this and (5-2) that our proposition is established as soon as we verify that $\tilde{f}\xi$ is a polarization. But there is a positive integer s such that $\zeta = s\sigma\xi$ is in $\mathbb{O}$; and now it follows from Lemma 5.1 that $s\tilde{f}\xi = f\zeta$ is a polarization. So $\tilde{f}\xi$ is too; and this completes the proof. □

6. Preliminary estimates (ii)

We now deal with type II. This is harder because there are now many positive involutions on $D = \mathbb{Q} \otimes \mathrm{End}\, A$; even worse, the canonical involution ρ_0 is not among them. It is here that we need the considerations of Section 2 on quadratic forms.

But first we recall the isomorphism ϕ from $\mathbb{R} \otimes D$ to $\mathcal{M}_2(\mathbb{R})^m$ constructed in Lemma 4.3 from a given polarization on A. We already have Equation (4-4), where * denotes complex conjugate transposition extended to the m-fold product. We also need the following remarks.

Lemma 6.1. *For any δ in $\mathbb{R} \otimes D$ we have*

$$\phi(\rho_0(\delta)) = \phi(\delta)^a,$$

where $(-)^a$ denotes the adjoint involution extended to the m-fold product.

Proof. The involution ρ_0 on $\mathbb{R}\otimes D$ induces via ϕ an involution i on $\mathcal{M}=\mathcal{M}_2(\mathbb{R})^m$. Since $\delta+\rho_0(\delta)$, $\delta\rho_0(\delta)$ are both fixed by ρ_0, they are in the center for every δ in $\mathbb{R}\otimes D$. It follows that $X+i(X)$, $X\,i(X)$ are both in the center of $\mathcal{M}$ for every X in $\mathcal{M}$. From this we conclude with a simple calculation that $i(X)=X^a$ for every X, which is the assertion of the present lemma. □

For the next remark we recall the decomposition $D=K\oplus E$ of Section 3.

Lemma 6.2. *For any α,β,γ in E linearly independent over K, the quadratic form*

$$Q(x,y,z)=-(x\alpha+y\beta+z\gamma)^2$$

has total signature $(+--)$.

Proof. Fix rational numbers x,y,z; then

$$q=Q(x,y,z)=\pi\rho_0(\pi)$$

for $\pi=x\alpha+y\beta+z\gamma$, so calculating $\phi_i(q)$ from both Lemma 4.3 and 6.1 using $MM^a=(\det M)I(2)$ on $\mathcal{M}_2(\mathbb{R})$ shows that

$$Q^{\phi_i}(x,y,z)=\det\phi_i(\pi)=\det(x\phi_i(\alpha)+y\phi_i(\beta)+z\phi_i(\gamma))\quad(1\le i\le m).$$

Since α,β,γ are linearly independent over K, their images in $\mathbb{R}\otimes D$ are linearly independent over $\mathbb{R}\otimes K$ and so their images by each ϕ_i in $\mathcal{M}_2(\mathbb{R})$ are linearly independent over $\mathbb{R}$. Further their traces are zero, again by Lemma 6.1. But it is easy to check that the determinant function evaluated on the zero trace subspace of $\mathcal{M}_2(\mathbb{R})$ has signature $(+--)$. The assertion of the present lemma is now evident, and this completes the proof. □

Although ρ_0 itself is not positive, it is known that every positive involution ρ on D is defined by

$$\rho(\delta)=\omega^{-1}\rho_0(\delta)\omega, \tag{6-1}$$

where ω is a nonzero element of D with ω^2 in K and totally negative (see, for example, [Lange and Birkenhake 1992, Theorem 5.3, p. 135], [Mumford 1974, Theorem 2, p. 201] or [Shimura 1963, Proposition 2, p. 153]). A simple calculation shows that ω lies in E (not K). Let $\Omega\subseteq E$ be the set of such elements ω. Our first task is to find a small element of Ω in the order $\mathbb{O}_1$. We keep the notation (5-1).

Lemma 6.3. *There exists $\tilde{\omega}$ in $\Omega\cap\mathbb{O}_1$ with*

$$|N(\tilde{\omega})|\le 2^{6m}|d_1(\mathbb{O}_1)|^3.$$

Proof. Write $M_1=E\cap\mathbb{O}_1$. By Lemma 3.2(b) we have

$$|d_1(M_1)|\le 2^{4m}|d_1(\mathbb{O}_1)|. \tag{6-2}$$

Now M_1 is an $\mathbb{O}$-module of rank 3, so by the definition of the generalized class index in [Masser and Wüstholz 1995a, p. 8] it contains a free $\mathbb{O}$-module $M = \mathbb{O}\alpha \oplus \mathbb{O}\beta \oplus \mathbb{O}\gamma$ with index $[M_1 : M] \le i_3(\mathbb{O})$. By the class index lemma we have $i_3(\mathbb{O}) \le d(\mathbb{O})^{3/2}$, and it follows using (3-5) and (6-2) that

$$|d_1(M)| = [M_1 : M]^2 |d_1(M_1)| \le 2^{-2m} d_1(\mathbb{O})^3 |d_1(\mathbb{O}_1)|.$$

So by Lemma 3.1 the quadratic form

$$Q(x, y, z) = -(x\alpha + y\beta + z\gamma)^2$$

satisfies

$$|N(d(Q))| \le 2^{-2m} |d_1(\mathbb{O}_1)|. \tag{6-3}$$

And by Lemma 6.2 it has total signature $(+--)$. So Lemma 2.6 provides ξ, η, ζ in $\mathbb{O}$ such that $q = -\tilde{\omega}^2$ is totally positive for $\tilde{\omega} = \xi\alpha + \eta\beta + \zeta\gamma$ in $\mathbb{O}_1$; and by (6-3)

$$N(q) \le 2^{4m/3} d(\mathbb{O})^5 |d_1(\mathbb{O}_1)|^{1/3}.$$

Finally the desired estimate for $|N(\tilde{\omega})| = N(q)^{1/2}$, even with exponent $\frac{8}{3}$, follows from this together with (3-5) and Lemma 3.2(a); the proof is thereby complete. □

We next give an analogue of Lemma 5.1; recall from Section 3 that tr is the reduced trace from D to K.

Lemma 6.4. *Suppose that f in* Pol A *has Rosati involution ρ given by (6-1) for some ω in Ω.*

(a) *Then $f_0 = f\omega^{-1}$ is in $\mathbb{Q} \otimes \mathcal{S}$, and we have*

$$f_0^{-1} \hat{\delta} f_0 = \rho_0(\delta) \tag{6-4}$$

for every δ in D.

(b) *Suppose further that ω' is in Ω. Then* $\operatorname{tr} \epsilon \ne 0$ *for $\epsilon = \omega^{-1}\omega'$.*

(c) *Suppose in addition that ϵ is in $\mathbb{O}_1$ with* tr ϵ *totally positive. Then $f\epsilon$ is in* Pol A.

Proof. By the definition (4-3) of ρ we have

$$f^{-1} \hat{\delta} f = \omega^{-1} \rho_0(\delta) \omega \tag{6-5}$$

for every δ in D. Put $\delta = \omega$; we get $f^{-1}\hat{\omega} f = -\omega$, and using $\hat{f} = f$ we see easily that the dual of f_0 satisfies $\hat{f}_0 = -f_0$. So f_0 is in $\mathbb{Q} \otimes \mathcal{S}$ as desired. Also the formula (6-4) is immediate from (6-5). This establishes (a).

As for (b), we fix $\phi = (\phi_1, \dots, \phi_m)$ corresponding to f as in Lemma 4.3, and we start by proving that the matrices

$$E_i = \phi_i(\epsilon) \quad (1 \le i \le m)$$

in $\mathcal{M}_2(\mathbb{R})$ are symmetric. For (4-4) gives the relations

$$\phi_i\big(\omega^{-1}\rho_0(\epsilon)\omega\big) = \phi_i(\epsilon)^t \quad (1 \le i \le m).$$

Also $\rho_0(\epsilon) = \omega'\omega^{-1}$, and we end up with the desired symmetry properties.

Next by Lemma 6.1 we have

$$(\det E_i) I = \phi_i(\epsilon)\phi_i(\rho_0(\epsilon)) = \phi_i\big(\omega^{-1}\omega'\omega'\omega^{-1}\big) \quad (1 \le i \le m)$$

for $I = I(2)$. But $\omega^2 = \sigma$ and $\omega'^2 = \sigma'$ are both totally negative in K; thus $\omega^{-1}\omega'\omega'\omega^{-1} = \sigma^{-1}\sigma'$ is totally positive in K, and the above matrix is $(\sigma^{-1}\sigma')^{\phi_i} I$. We deduce that

$$\det E_i > 0 \quad (1 \le i \le m). \tag{6-6}$$

If t_i is the trace of E_i, then we also have

$$t_i I = \phi_i(\epsilon) + \phi_i(\rho_0(\epsilon)) = 2\phi_i(\tau) = 2\tau^{\phi_i} I \quad (1 \le i \le m) \tag{6-7}$$

with $\tau = \operatorname{tr}\epsilon$ the reduced trace. Now $\tau = 0$ would imply $t_i = 0$ $(1 \le i \le m)$, but the trace of a symmetric matrix in $\mathcal{M}_2(\mathbb{R})$ cannot vanish if its determinant is positive as in (6-6). So indeed $\tau \ne 0$, and this establishes (b).

Lastly, suppose τ is totally positive. We prove that $E_1, \dots, E_m$ are positive definite. For (6-7) now implies that $t_i > 0$ $(1 \le i \le m)$, and it is easy to check that a symmetric matrix in $\mathcal{M}_2(\mathbb{R})$ is positive definite if (and only if) its determinant and trace are both positive. Thus $E_1, \dots, E_m$ are indeed positive definite.

Finally from Lemma 4.5 we know that the polarization f corresponds to the form $z^t F \bar{w}$ with

$$F = \operatorname{diag}(F_1, \dots, F_m),$$

where $F_i = I \otimes F_i'$ for F_i' of order $n/2m$ $(1 \le i \le m)$. As in the proof of Lemma 5.1, the map $f\epsilon$ corresponds to $z^t F_\epsilon \bar{w}$ with $F_\epsilon = \Phi(\epsilon)^t F$, and we have

$$\Phi(\epsilon) = \operatorname{diag}(\Phi_1(\epsilon), \dots, \Phi_m(\epsilon))$$

with $\Phi_i(\epsilon) = E_i \otimes I'$ $(1 \le i \le m)$ for $I' = I(n/2m)$. By symmetry we get

$$\Phi_i(\epsilon)^t F_i = (E_i \otimes I')(I \otimes F_i') = E_i \otimes F_i' \quad (1 \le i \le m),$$

so that

$$F_\epsilon = \operatorname{diag}(E_1 \otimes F_1', \dots, E_m \otimes F_m').$$

Since F is positive definite Hermitian, so are $F_1, \dots, F_m$ and also $F_1', \dots, F_m'$. We have just seen that $E_1, \dots, E_m$ are positive definite Hermitian (and even symmetric). Now it is well known (and almost trivial) that the Kronecker product of two positive definite Hermitian matrices is also positive definite Hermitian. It follows that F_ϵ is

positive definite Hermitian, and so $f\epsilon$ is a polarization. This establishes (c), and so completes the proof of the present lemma. □

The next result is the analogue of Lemma 5.2, but with the Néron–Severi group replaced by the Severi–Néron group.

Lemma 6.5. *The group* $\mathcal{S} = \mathrm{SN}(A)$ *is a right* $\mathbb{O}$*-module of rank* 1; *the group* $\mathcal{S}' = \mathrm{SN}(\hat{A})$ *is a left* $\mathbb{O}$*-module of rank* 1; *and* $f'f$ *is in* $\mathbb{O}$ *for every* f *in* $\mathcal{S}$ *and* f' *in* $\mathcal{S}'$.

Proof. The claims for $\mathcal{S}$ can be checked by noncanonical identification, as in the proof of Lemma 5.2. In fact a Rosati involution of the form (6-1) has antifixed space $K\omega$, since the equation $\rho(\delta\omega) = -\delta\omega$ turns out to be equivalent to $\rho_0(\delta) = \delta$. So $\mathcal{H}$, $\mathcal{N}$, $\mathcal{S}$ have $\mathbb{Z}$-ranks $4m$, $3m$, m, respectively. The claims for $\mathcal{S}'$ can be verified similarly.

Finally let f be in $\mathcal{S}$ and f' in $\mathcal{S}'$. In showing that $f'f$ is in $\mathbb{O}$ we can assume $f \neq 0$. By Lemma 6.4(a) applied to some polarization (of course not the present f) there is some f_0 in $\mathbb{Q} \otimes \mathcal{S}$ with $f_0^{-1}\hat{\delta} f_0 = \rho_0(\delta)$ for every δ in D. Since $f_0 = f\sigma$ for some σ in K, we deduce also

$$f^{-1}\hat{\delta} f = \rho_0(\delta) \tag{6-8}$$

for every δ in D. With $\delta = f'f$ using $\hat{f} = -f$ and a similar equation for f' leads immediately to $f'f = \rho_0(f'f)$, so $f'f$ is in K and therefore in $\mathbb{O}$ as desired. This completes the proof. □

It is perhaps interesting to note that (6-8) above says that any nonzero f in $\mathcal{S}$ (for type II) determines the canonical involution on D in the same way as a polarization determines its Rosati involution (compare (4-3)).

We now establish our second preliminary estimate for polarizations.

Proposition 6.6. *Suppose that* A *is simple and its endomorphism algebra is a totally indefinite quaternion algebra over a totally real number field. Then* A *has a polarization of degree at most*

$$2^{30mn} c(\mathcal{H}', \mathcal{H})^n |d_1(\mathbb{O}_1)|^{7n}.$$

Proof. From Lemma 4.1(b) we have $c(\mathcal{S}', \mathcal{S}) \neq 0$. Lemma 6.5 allows us to apply Lemma 4.2 with $\Gamma = \mathcal{S}$, $\Gamma' = \mathcal{S}'$ to find an isogeny $\tilde{f}$ in $\mathcal{S}$ with $\deg \tilde{f} \leq c(\mathcal{S}', \mathcal{S})^n$. Again using Lemma 4.1(b) and $\ell = 4m$, we get

$$\deg \tilde{f} \leq 2^{16mn} c(\mathcal{H}', \mathcal{H})^n. \tag{6-9}$$

Next by Lemma 6.3 there is $\tilde{\omega}$ in $\Omega \cap \mathbb{O}_1$ with $|N(\tilde{\omega})| \leq 2^{6m} |d_1(\mathbb{O}_1)|^3$, and therefore

$$\deg \tilde{\omega} = |N(\tilde{\omega})|^{2n/m} \leq |N(\tilde{\omega})|^{2n} \leq 2^{12mn} |d_1(\mathbb{O}_1)|^{6n}. \tag{6-10}$$

Now there is certainly some polarization f, and the Rosati involution for f has the form (6-1) for some ω in Ω. By Lemma 6.4(a), $f_0 = f\omega^{-1}$ lies in $\mathbb{Q} \otimes \mathcal{S}$, and therefore $\tilde{f} = f_0\sigma$ for some nonzero σ in K. By Lemma 6.4(b), $\tau = \mathrm{tr}(\omega^{-1}\tilde{\omega})$ is nonzero and so we can use Lemma 2.1 to find ξ in $\mathbb{O}$ such that $\sigma\tau\xi$ is totally positive and $|N(\xi)| \le d(\mathbb{O})^{1/2}$. Exactly as in (5-3) above we find

$$\deg \xi \le 2^{2mn} |d_1(\mathbb{O}_1)|^n.$$

Now it is clear from this and (6-9), (6-10) that the proposition is established as soon as we verify that $\tilde{f}\tilde{\omega}\xi$ is a polarization. But there is a positive integer s such that $\epsilon = \omega^{-1}\omega'$ is in $\mathbb{O}_1$ for $\omega' = s(\tilde{\omega}\sigma\xi)$, and by construction $\mathrm{tr}\,\epsilon = s(\sigma\tau\xi)$ is totally positive. So from Lemma 6.4(c) we see that $f\epsilon = s(\tilde{f}\tilde{\omega}\xi)$ is a polarization. So $\tilde{f}\tilde{\omega}\xi$ is too; and this completes the proof. □

7. Conclusion

We prove the theorem first. Thus let A be a simple abelian variety of dimension n whose endomorphism algebra is commutative or has the property that its center is totally real of degree m. Then we are in the situation of Section 5 or 6, and the appropriate proposition shows that A has a polarization of degree at most

$$2^{30mn} c(\mathcal{H}', \mathcal{H})^n |d_1(\mathbb{O}_1)|^{7n}, \tag{7-1}$$

where $\mathcal{H} = \mathrm{Hom}(A, \hat{A})$, $\mathcal{H}' = \mathrm{Hom}(\hat{A}, A)$ and $\mathbb{O}_1 = \mathrm{End}\, A$.

Now suppose that A is defined over a number field of degree d. We use positive constants $C_1, C_2, \ldots$ depending only on n and d, and we estimate the quantities in (7-1) in terms of $h = \max\{1, h(A)\}$ using Lemma 6.1 of [Masser and Wüstholz 1995a, p. 19]; this says that

$$\max\{c(\mathcal{H}', \mathcal{H}), |d_1(\mathbb{O}_1)|\} \le C_1 h^\lambda,$$

where $\lambda = \lambda(8n)$ for a certain monotonically increasing function. The inequality of our theorem follows immediately, with exponent $8n\lambda(8n)$.

To prove the first corollary, we note that if A is simple of squarefree dimension n then its endomorphism algebra D is necessarily of the form considered in the theorem. For we only have to rule out the noncommutative case of type IV. In this case D has dimension $e^2 \ge 4$ over its center, which is a CM-field of degree $2m$. Now it is well known that the $\mathbb{Q}$-dimension $2me^2$ of D must divide $2n$ (see [Lange and Birkenhake 1992, Proposition 5.7, p. 141] or [Mumford 1974, p. 182]). This is here impossible and so the first corollary is proved.

Similarly, as preparation for the proof of the second corollary, we note that if A is simple of dimension $n \le 7$ then D is also as in the theorem. Here the only possibility is $e^2 = 4$ and then $m = 1$, $n = 4$.

Now it is a fact that such a case is impossible for simple A, but we could not find a completely satisfactory explicit reference in the literature. Without using this fact, the second corollary would follow only for dimension n at most 3. So we feel obliged to add some remarks about the impossible case.

Everything can be found in Albert's papers [1934a; 1935a], but the reader may well appreciate a more modern exposition. There are two subcases characterized by $r_1 s_1 = 0$ and $r_1 s_1 \neq 0$. The first of these is covered by [Albert 1934a, Theorem 3, p. 13]. A modern treatment (which also implies that A is isogenous to the fourth power of a CM elliptic curve) is given in Shimura [1963, Proposition 14, p. 176]. See [Lange and Birkenhake 1992, Exercise 3, p. 286].

Next if $r_1 s_1 \neq 0$ then $r_1 = s_1 = 1$ by virtue of $r_1 + s_1 = 2$. So this subcase is covered by [Albert 1935a, Theorem 20, p. 391] and also [Shimura 1963, Proposition 19, p. 184]. However Shimura's conclusion that A is isogenous to the square of an abelian surface (of endomorphism type II with $m = 1$) is valid only for what he calls "generic" A; his arguments are definitely moduli-space-theoretic in nature. Our own A is defined over a number field and so unlikely to be generic; on the other hand it is known that specialization only increases the endomorphism ring. Now the generic ring already has rank 16 over $\mathbb{Z}$, whereas the maximum rank for simple A of dimension 4 is only 8 (see above). A general result independent of such considerations is given in [Lange and Birkenhake 1992, Exercise 5, p. 286].

This last subcase $r_1 = s_1 = 1$ can also be treated using only a very elementary specialization argument, paying due attention to the discrepancy between Shimura's analytic concept of generic and the more usual algebraic concept. We omit the details.

We now prove the second corollary. Suppose first that A is an abelian variety of dimension n, not necessarily simple, defined over a number field k of degree d. By [Masser and Wüstholz 1995a, Theorem I, p. 5] there are abelian subvarieties $A_1, \ldots, A_r$ of A, simple over the algebraic closure $\bar{k}$, together with an isogeny g from A to $A' = A_1 \times \cdots \times A_r$ of degree

$$\deg g \leq C_2 h^{\kappa} \tag{7-2}$$

for $\kappa = \kappa(n)$ depending only on n. Also, as in [Masser and Wüstholz 1995a, p. 6], $A_1, \ldots, A_r$ are necessarily defined over an extension of k of relative degree at most C_3. Assume that the endomorphism algebras of $A_1, \ldots, A_r$ are all of the type considered in our theorem. As we have observed, this is automatically true if $n \leq 7$. Then A_i has a polarization f_i of degree at most $C_4 \max\{1, h(A_i)\}^{8n_i\lambda}$, where λ is as above and n_i is the dimension of A_i $(1 \leq i \leq r)$. As in [Masser and Wüstholz 1995a, p. 6] we have $h(A) \leq C_5 h$ $(1 \leq i \leq r)$, and so

$$\deg f_i \leq C_6 h^{8n_i\lambda} \quad (1 \leq i \leq r).$$

Therefore $A' = \prod A_i$ has a polarization f with

$$\deg f = \prod (\deg f_i) \le C_7 h^{8n\lambda}. \tag{7-3}$$

Finally the "pullback" $\hat{g} f g$ is a polarization on A whose degree is $(\deg g)^2 (\deg f)$. So by (7-2) and (7-3) this completes the proof of the second corollary, with exponent $8n\lambda(8n) + 2\kappa(n)$.

References

[Albert 1934a] A. A. Albert, "On the construction of Riemann matrices, I", *Ann. of Math.* (2) **35**:1 (1934), 1–28. MR 1503140 Zbl 0010.00304

[Albert 1934b] A. A. Albert, "A solution of the principal problem in the theory of Riemann matrices", *Ann. of Math.* (2) **35**:3 (1934), 500–515. MR 1503176 Zbl 0010.00401

[Albert 1935a] A. A. Albert, "On the construction of Riemann matrices, II", *Ann. of Math.* (2) **36**:2 (1935), 376–394. MR 1503230 Zbl 0011.38904

[Albert 1935b] A. A. Albert, "Involutorial simple algebras and real Riemann matrices", *Ann. of Math.* (2) **36**:4 (1935), 886–964. MR 1503260 Zbl 0012.39102

[Baker and Wüstholz 2007] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, New Mathematical Monographs **9**, Cambridge University Press, 2007. MR 2009e:11001 Zbl 1145.11004

[Bost 1996a] J.-B. Bost, "Intrinsic heights of stable varieties and abelian varieties", *Duke Math. J.* **82**:1 (1996), 21–70. MR 97j:14025 Zbl 0867.14010

[Bost 1996b] J.-B. Bost, "Périodes et isogénies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz)", pp. 115–161 in *Séminaire Bourbaki*, Astérisque **237**, Société Mathématique de France, Paris, 1996. MR 98k:11073 Zbl 0936.11042

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR 85g:11026a Zbl 0588.14026

[Gaudron and Rémond 2013] É. Gaudron and G. Rémond, "Polarisations et isogénies", preprint, 2013, http://math.univ-bpclermont.fr/∼gaudron/art13.pdf.

[Gruber and Lekkerkerker 1987] P. M. Gruber and C. G. Lekkerkerker, *Geometry of numbers*, 2nd ed., North-Holland Mathematical Library **37**, North-Holland, Amsterdam, 1987. MR 88j:11034 Zbl 0611.10017

[Howe 1995] E. W. Howe, "Bounds on polarizations of abelian varieties over finite fields", *J. Reine Angew. Math.* **467** (1995), 149–155. MR 96i:11064 Zbl 0832.14033

[Lange and Birkenhake 1992] H. Lange and Ch.. Birkenhake, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften **302**, Springer, Berlin, 1992. MR 94j:14001 Zbl 0779.14012

[Masser 2006] D. W. Masser, "From $2^{\sqrt{2}}$ to polarizations on abelian varieties", pp. 37–43 in *Colloquium De Giorgi 2006*, edited by U. Zannier, Colloquia **1**, Edizione della Normale, Pisa, 2006. MR 2008m:14086 Zbl 1231.11081

[Masser and Wüstholz 1993a] D. W. Masser and G. Wüstholz, "Periods and minimal abelian subvarieties", *Ann. of Math.* (2) **137**:2 (1993), 407–458. MR 94g:11040 Zbl 0796.11023

[Masser and Wüstholz 1993b] D. W. Masser and G. Wüstholz, "Isogeny estimates for abelian varieties, and finiteness theorems", *Ann. of Math.* (2) **137**:3 (1993), 459–472. MR 95d:11074 Zbl 0804.14019

[Masser and Wüstholz 1993c] D. W. Masser and G. Wüstholz, "Galois properties of division fields of elliptic curves", *Bull. London Math. Soc.* **25**:3 (1993), 247–254. MR 94d:11036 Zbl 0809.14026

[Masser and Wüstholz 1994] D. W. Masser and G. Wüstholz, "Endomorphism estimates for abelian varieties", *Math. Z.* **215**:4 (1994), 641–653. MR 95b:14032 Zbl 0826.14025

[Masser and Wüstholz 1995a] D. W. Masser and G. Wüstholz, "Factorization estimates for abelian varieties", *Inst. Hautes Études Sci. Publ. Math.* **81** (1995), 5–24. MR 96j:11083 Zbl 0854.11030

[Masser and Wüstholz 1995b] D. W. Masser and G. Wüstholz, "Refinements of the Tate conjecture for abelian varieties", pp. 211–224 in *Abelian varieties* (Egloffstein, 1993), edited by W. Barth et al., de Gruyter, Berlin, 1995. MR 97a:11092 Zbl 0876.14029

[Mumford 1974] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Oxford University Press, London, 1974. MR 44 #219 Zbl 0223.14022

[Reiner 1975] I. Reiner, *Maximal orders*, London Mathematical Society Monographs **5**, Academic Press, London, 1975. Corrected reprint published by Oxford Univ. Press, 2003. MR 52 #13910 Zbl 0305.16001

[Shimura 1963] G. Shimura, "On analytic families of polarized abelian varieties and automorphic functions", *Ann. of Math.* (2) **78** (1963), 149–192. MR 27 #5934 Zbl 0142.05402

Communicated by John Henry Coates
Received 2013-04-22 Revised 2013-12-13 Accepted 2014-02-15

David.Masser@unibas.ch *Mathematisches Institut, Universität Basel, CH-4051 Basel, Switzerland*

gisbert.wuestholz@math.ethz.ch *Departement für Mathematik, ETH-Zentrum, CH-8092 Zürich, Switzerland*

Algebra & Number Theory

msp.org/ant

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 8 No. 5 2014