

ON COMPATIBILITY BETWEEN ISOGENIES AND POLARIZATIONS OF ABELIAN VARIETIES

MARTIN ORR

ABSTRACT. We discuss the notion of polarized isogenies of abelian varieties, that is, isogenies which are compatible with given principal polarizations. This is motivated by problems of unlikely intersections in Shimura varieties. Our aim is to show that certain questions about polarized isogenies can be reduced to questions about unpolarized isogenies or vice versa.

Our main theorem concerns abelian varieties B which are isogenous to a fixed abelian variety A . It establishes the existence of a polarized isogeny $A \rightarrow B$ whose degree is polynomially bounded in n , if there exist both an unpolarized isogeny $A \rightarrow B$ of degree n and a polarized isogeny $A \rightarrow B$ of unknown degree. As a further result, we prove that given any two principally polarized abelian varieties related by an unpolarized isogeny, there exists a polarized isogeny between their fourth powers.

The proofs of both theorems involve calculations in the endomorphism algebras of the abelian varieties, using the Albert classification of these endomorphism algebras and the classification of Hermitian forms over division algebras.

1. INTRODUCTION

The goal of this paper is to prove some results about the existence of polarized isogenies between abelian varieties, motivated by work on the André–Pink conjecture on unlikely intersections. The endomorphism algebra of an abelian variety is a semisimple \mathbb{Q} -algebra with involution, and polarizations of the abelian variety correspond to positive definite Hermitian forms over this algebra. Hence most of the paper is in fact concerned with isometries of Hermitian forms over such algebras.

1.1. Abelian varieties, isogenies and polarizations. We begin by recalling a number of definitions: isogenies and polarizations of abelian varieties, and the notion of polarized isogenies which are the objects of our main theorems.

An **abelian variety** is a complete algebraic variety equipped with multiplication and inverse maps which make it into a group object in the category of algebraic varieties over some field. For the purposes of this paper, it does not matter what the base field is (algebraically closed or not, positive characteristic or characteristic zero). See [Mum70] and [Mil86] for the main results about abelian varieties.

2010 *Mathematics Subject Classification.* 11E39, 14K02.

Key words and phrases. Abelian varieties, isogenies, polarizations, Hermitian forms.

An **isogeny** is a homomorphism of abelian varieties which is surjective and finite as a morphism of varieties. The relation “there exists an isogeny from A to B ” is an equivalence relation on abelian varieties, a bit weaker than isomorphism, which preserves many geometric and arithmetic invariants, for example the endomorphism algebra of the abelian variety. The **degree** of an isogeny is its degree as a morphism of varieties.

A **polarization** of an abelian variety A is an isogeny $A \rightarrow A^\vee$ (where A^\vee is the dual abelian variety) which is induced by an ample line bundle on $A_{\bar{k}}$ according to a certain recipe, whose details are not important here. We say that a polarization is **principal** if it has degree 1. Every abelian variety possesses at least one polarization, but not always a principal polarization. A **principally polarized abelian variety** is a pair (A, λ) consisting of an abelian variety A and a principal polarization λ of A .

The **endomorphism ring** $\text{End } A$ of an abelian variety A is the ring of homomorphisms $A \rightarrow A$. Note that $\text{End } A$ may be strictly smaller than the endomorphism ring of $A_{\bar{k}}$. The **endomorphism algebra** of A is $\text{End } A \otimes_{\mathbb{Z}} \mathbb{Q}$. The endomorphism algebra is a semisimple algebra over \mathbb{Q} (whatever the base field of A) and the endomorphism ring is an order in this algebra. Any polarization of A induces a positive involution, called the **Rosati involution**, of $\text{End } A \otimes_{\mathbb{Z}} \mathbb{Q}$. If the polarization is principal, then the Rosati involution maps $\text{End } A$ into itself.

Let (A, λ) and (B, μ) be principally polarized abelian varieties. If $f: A \rightarrow B$ is an isogeny, then we obtain a polarization $f^*\mu$ on A , given by $f^\vee \circ \mu \circ f$, or equivalently, the polarization induced by the line bundle $f^*\mathcal{M}$ on A if \mathcal{M} is a line bundle on B inducing μ .

We then say that f is a **polarized isogeny**, or that it is **compatible with the polarizations**, if

$$f^*\mu = n.\lambda \text{ for some } n \in \mathbb{Z}.$$

Note that it would be too strict to require in this definition that

$$f^*\mu = \lambda$$

because $f^*\mu$ has degree $(\deg f)^2$, so this equality can only hold if $\deg f = 1$, that is, if f is an isomorphism.

One motivation for considering polarizations is that we can construct a moduli space \mathcal{A}_g of principally polarized abelian varieties of dimension g , but not a moduli space of unpolarized abelian varieties. This moduli space is an example of a Shimura variety.

The significance of polarized isogenies then lies in the fact that two principally polarized abelian varieties are related by a polarized isogeny if and only if the corresponding points of \mathcal{A}_g lie in the same Hecke orbit. Hecke orbits are natural equivalence classes on Shimura varieties.

1.2. Polarized versus unpolarized isogeny classes. The relation “there exists a polarized isogeny from (A, λ) to (B, μ) ” is an equivalence relation on polarized abelian varieties which is stronger than the existence of an isogeny from A to B (forgetting the polarizations). Proposition 3.1 gives an example in which the polarized isogeny class of a principally polarized abelian variety is strictly smaller than its unpolarized isogeny class (namely, an abelian surface with multiplication by a real quadratic field).

Our first main result (section 4) shows that the existence of an unpolarized isogeny between two principally polarized abelian varieties *does* imply the existence of a polarized isogeny between their fourth powers. Thus some questions about abelian varieties in an isogeny class can be reduced to questions about abelian varieties in a polarized isogeny class (which may be more natural if one is looking at the moduli space of principally polarized abelian varieties), by replacing the original varieties by their fourth powers.

Theorem 1.1. *Let (A, λ) and (B, μ) be principally polarized abelian varieties over the same base field. If A and B are isogenous, then there is a polarized isogeny from $(A, \lambda)^4$ to $(B, \mu)^4$.*

In the proof of Theorem 1.1, we begin by reducing to the case in which A is **isotypic**, that is, isogenous to A_0^r for some simple abelian variety A . If D is the endomorphism algebra of A_0 , then the polarizations λ and $f^*\mu$ induce positive definite Hermitian forms ψ_1 and ψ_2 on D^r . In order to show that there is a polarized isogeny from $(A, \lambda)^4$ to $(B, \mu)^4$, we have to show that the direct sum of four copies of ψ_1 is isometric to a rational multiple of the direct sum of four copies of ψ_2 . In fact we prove that the previous sentence holds without the words “a rational multiple of.”

Theorem 1.2. *Let $(D, *)$ be a division algebra over \mathbb{Q} with a positive involution. Let V be a finite-dimensional right D -module and let*

$$\psi_1, \psi_2: V \times V \rightarrow D$$

*be two positive definite $(D, *)$ -Hermitian forms.*

Then $\psi_1^{\oplus 4}$ and $\psi_2^{\oplus 4}$ are isometric.

We prove Theorem 1.2 by breaking it into cases using the Albert classification of division algebras with positive involution, then using the classification of $(D, *)$ -Hermitian forms from chapter 10 of [Sch85] in each case. For division algebras of Albert types I, III and IV, isometry of Hermitian forms satisfies a local-global principle so this classification is straightforward. For division algebras of type II, the isometry class of a Hermitian form is not determined by its localizations, so we must use a result of Lewis [Lew82] describing the obstruction to the local-global principle.

1.3. A degree bound for polarized isogenies. Our second main theorem (section 5) asserts that, if we fix a principally polarized abelian variety (A, λ) and consider any other principally polarized abelian variety (B, μ) in the same polarized isogeny class such that we know the degree n of an unpolarized isogeny $A \rightarrow B$, then A and B are related by a polarized isogeny whose degree is bounded by a polynomial in n .

Theorem 1.3. *Let (A, λ) be a principally polarized abelian variety over a field K . There exist constants c and k , depending on (A, λ) , such that:*

If (B, μ) is a principally polarized abelian variety over K for which

- (1) there exists a polarized isogeny $f: A \rightarrow B$ (of any degree), and*
- (2) there exists an isogeny $g: A \rightarrow B$ of degree n (not necessarily polarized),*

then there exists a polarized isogeny $h: A \rightarrow B$ of degree at most cn^k .

The constant k can be chosen to be $4 \dim A$, while the constant c depends on the endomorphism ring of A .

Note that it is obvious, under conditions (1) and (2), that there exists a polarized isogeny $h: A \rightarrow B$ whose degree is bounded by some function $C(A, \lambda, n)$. This is because there are only finitely many abelian varieties related to A by an isogeny of degree n , and each of them has only finitely many principal polarizations (up to polarized isomorphism of principally polarized abelian varieties), by [Mil86] Theorem 18.1. The content of Theorem 1.3 is that this bound is polynomial in n .

Theorem 1.3 is particularly useful in combination with the Masser–Wüstholz isogeny theorem. If we fix an abelian variety A over a number field and consider abelian varieties B over larger number fields such that $A_{\bar{K}}$ is isogenous to $B_{\bar{K}}$, the Masser–Wüstholz theorem asserts that there exists an isogeny $A_{\bar{K}} \rightarrow B_{\bar{K}}$ whose degree is bounded by a polynomial in the degree of the field of definition of B . The relevant part of the Masser–Wüstholz theorem is as follows.

Theorem 1.4 ([MW93]). *Let K be a number field and A a principally polarized abelian variety over K . There exist constants c and κ , depending on A and K , such that:*

If B is any principally polarized abelian variety over a finite extension L of K such that $A_{\bar{K}}$ is isogenous to $B_{\bar{K}}$, then there exists an isogeny $A_{\bar{K}} \rightarrow B_{\bar{K}}$ of degree at most

$$c(A, K)[L : K]^{\kappa}.$$

The isogeny of bounded degree whose existence is asserted by Theorem 1.4 is not necessarily a polarized isogeny, even if we know initially that $A_{\bar{K}}$ and $B_{\bar{K}}$ are in the same polarized isogeny class. Combining Theorems 1.3 and 1.4 establishes that, in the setting of Theorem 1.4, if $(B_{\bar{K}}, \mu)$ is in the *polarized* isogeny class of $(A_{\bar{K}}, \lambda)$, then there exists a *polarized* isogeny $A_{\bar{K}} \rightarrow B_{\bar{K}}$ satisfying a bound of the same form as Theorem 1.4.

1.4. Proof of the degree bound. The proof of Theorem 1.3 is easily reduced to a result about endomorphisms of an abelian variety. We begin by outlining the idea of this proof in the case of an isotypic abelian variety. As mentioned above, in the isotypic case the polarizations λ and $g^*\mu$ of A induce positive definite Hermitian forms ψ_1 and ψ_2 on D^r for a suitable division algebra D and $r \in \mathbb{N}$. The degree n of g controls the determinants of these forms on a suitable lattice Λ in D^r . The existence of a polarized isogeny f implies that ψ_2 is isometric to a rational scalar multiple of ψ_1 . In order to prove the existence of a polarized isogeny h of bounded degree, we have to show that there is an isometry from ψ_2 to a rational scalar multiple of ψ_1 which maps Λ into itself and whose determinant is bounded by a polynomial in n .

However, it seems difficult to reduce the non-isotypic case of Theorem 1.3 to the isotypic case. The problem is that if

$$f_1: (A_1, \lambda_1) \rightarrow (B_1, \mu_1), \quad f_2: (A_2, \lambda_2) \rightarrow (B_2, \mu_2)$$

are polarized isogenies, then we only know that

$$(f_1, f_2)^*(\mu_1, \mu_2) = (n_1\lambda_1, n_2\lambda_2)$$

for some integers n_1 and n_2 , but n_1 might not be equal to n_2 , and so (f_1, f_2) might not be a polarized isogeny.

We have found it more convenient to write most of the argument using a symmetric element $q \in E$ (where E is a semisimple algebra) instead of Hermitian forms over the simple factors of E . In the following proposition, the hypothesis that there exists a such that $a^\dagger qa \in \mathbb{Q}^\times$ corresponds to condition (1) in Theorem 1.3 while $N_E(q)$ is related to the degree of g as appears in condition (2) of Theorem 1.3.

Proposition 1.5. *Let (E, \dagger) be a semisimple \mathbb{Q} -algebra with involution, let $R \subset E$ be a \dagger -stable order, and let N_E be a \dagger -compatible norm on E of rank d .*

There exists a constant c depending only on (R, \dagger, N_E) such that:

For every $q \in R$, if there exists $a \in E$ such that $a^\dagger qa \in \mathbb{Q}^\times$, then there exists $b \in R$ such that

$$b^\dagger qb \in \mathbb{Z} - \{0\} \text{ and } N_E(b) \leq c N_E(q)^{d-1/2}.$$

The proof of Proposition 1.5 uses a local-to-global approach. First we prove that the proposition itself holds for the localization of the algebra E at each rational prime p , with a constant c_p depending on p . This part of the proof uses Benoist and Oh's p -adic polar decomposition [BO07]. We then give an independent proof that for all but finitely many p , we can take $c_p = 1$. In the latter part of the proof, we use Hermitian forms as sketched above for the isotypic case, in particular the integral classification of Hermitian forms over local fields and Shimura's results on maximal lattices. We then use reduction theory for the adelic points of the multiplicative group of E to obtain a global result from these local results.

1.5. Application to the André–Pink conjecture. The results in this paper on the relationship between isogeny classes and polarized isogeny classes are related to the André–Pink conjecture. In particular, the results of this paper provide an alternative approach to some parts of the author’s recent work on the André–Pink conjecture [Orr15].

The André–Pink conjecture for \mathcal{A}_g is stated in Conjecture 1.6 below (the definition of “special subvariety” is not important for the present discussion). A key issue in studying this conjecture is the relationship between Conjecture 1.6 and the *a priori* slightly stronger Conjecture 1.7. Viewed from the perspective of Shimura varieties, the natural statement is Conjecture 1.6 – a generalization to arbitrary mixed Shimura varieties can be found at [Pin05] Conjecture 1.6. On the other hand, viewed from the perspective of abelian varieties, Conjecture 1.7 appears more natural.

Conjecture 1.6 (André–Pink). *Let Z be an irreducible algebraic subvariety of the moduli space \mathcal{A}_g of principally polarized abelian varieties of dimension g over \mathbb{C} .*

If there exists a polarized isogeny class Σ in \mathcal{A}_g such that $\Sigma \cap Z$ is Zariski dense in Z , then Z is a special subvariety of \mathcal{A}_g .

Conjecture 1.7. *Conjecture 1.6 holds with “a polarized isogeny class Σ ” replaced by “an isogeny class Σ .”*

In [Orr15], the author proved some cases of Conjecture 1.7. In particular, this includes the case when Z is a curve, and some partial progress on other cases.

Theorem 1.8. ([Orr15] *Theorem 1.2*) *Conjecture 1.7 holds when Z is a curve.*

The proof of Theorem 1.8 relies on the Masser–Wüstholz isogeny theorem and the Pila–Zannier method for solving unlikely intersections problems in Shimura varieties. The proof is complicated by the fact that a straightforward application of the Pila–Zannier method would only apply to polarized isogenies, while the Masser–Wüstholz theorem concerns unpolarized isogenies. In [Orr15], this is worked around by a more sophisticated application of the Pila–Zannier method, as discussed in [Orr15] section 3.2.

The results in this paper explore the relationship between polarized and unpolarized isogenies directly instead of bypassing it, and thereby give an alternative proof of Theorem 1.8. We can use Theorem 1.3 to replace most of the difficult parts of [Orr15], leading to a proof of Conjecture 1.6 for a curve Z . Theorem 1.1 allows us to deduce Conjecture 1.7 for a curve in \mathcal{A}_g from Conjecture 1.6 for a curve in \mathcal{A}_{4g} .

Nevertheless the proofs of the theorems in this paper are sufficiently complicated that the proof of Theorem 1.8 sketched above seems to be longer overall than the proof in [Orr15].

2. BACKGROUND: HERMITIAN FORMS AND INVOLUTIONS

Before the main proofs of this paper, we collect some basic facts about Hermitian forms over division algebras. We begin with some general definitions and facts, to fix the terminology and notation we will use, which is based on [KMRT98]. We then state results about two particular aspects of the theory of Hermitian forms: positive definite forms, using [Kot92], and lattices, using [Shi63] and [Shi97].

2.1. General Hermitian forms and involutions. Let $(D, *)$ be a simple algebra with involution. By an **involution**, we mean an additive map $D \rightarrow D$ whose square is the identity and which *reverses* the direction of multiplication. When we say **simple algebra with involution**, we include the case in which D is a product of two simple algebras $D_1 \times D_2$ and the involution exchanges the two factors (this is not simple as an algebra, but it is simple as an algebra-with-involution). The involution $*$ is said to be **of the first kind** if it is trivial on the centre of D , and **of the second kind** otherwise.

We say that an element $d \in D$ is **symmetric** if $d^* = d$.

Let V be a free right D -module of finite dimension. A $(D, *)$ -**Hermitian form** on V is a bi-additive map

$$\psi: V \times V \rightarrow D$$

satisfying

- (1) $\psi(va, wb) = a^*\psi(v, w)b$ for all $v, w \in V$ and $a, b \in D$, and
- (2) $\psi(w, v) = \psi(v, w)^*$ for all $v, w \in V$.

A $(D, *)$ -**skew-Hermitian form** on D^n is a bi-additive map satisfying condition (1) above and also $\psi(w, v) = -\psi(v, w)^*$.

A Hermitian or skew-Hermitian form is **non-singular** (also called **regular**) if the only element $v \in V$ such that $\psi(v, w) = 0$ for all $w \in V$ is $v = 0$.

Given any non-singular Hermitian or skew-Hermitian form $\psi: V \times V \rightarrow D$, there is a unique involution \dagger of $\text{End}_D(V)$, called the **adjoint involution** with respect to ψ , such that

$$\psi(av, w) = \psi(v, a^\dagger w)$$

for all $v, w \in V$ and $a \in \text{End}_D(V)$.

The following proposition shows that we can reverse the construction of adjoint involutions, passing from an involution to a Hermitian or skew-Hermitian form. This proposition is [KMRT98] Proposition I.4.2 whenever D is simple as an algebra (forgetting the involution), and it follows from [KMRT98] Proposition I.2.14 whenever D is a product of two simple algebras.

Proposition 2.1. *Let $(D, *)$ be a simple algebra with involution. Let V be a free right D -module of finite dimension.*

- (1) *If $*$ is of the first kind, then the map sending a form to its associated adjoint involution induces a bijection between*

- (a) *non-singular $(D, *)$ -Hermitian and $(D, *)$ -skew-Hermitian forms on V , modulo multiplication by an element of the centre of D , and*
 - (b) *involutions of $\text{End}_D(V)$ of the first kind.*
- (2) *If $*$ is of the second kind, then the map sending a form to its associated adjoint involution induces a bijection between*
- (a) *non-singular $(D, *)$ -Hermitian forms on V , modulo multiplication by an element of the centre of D which is fixed by $*$, and*
 - (b) *involutions \dagger of $\text{End}_D(V)$ such that $a^\dagger = a^*$ for all a in the centre of D .*

The natural notion of equivalence between Hermitian or skew-Hermitian forms is isometry. We say that two right D -modules V_1 and V_2 equipped with Hermitian or skew-Hermitian forms ψ_1 and ψ_2 respectively are **isometric** if there is an isomorphism of D -modules $f: V_1 \rightarrow V_2$ such that

$$\psi_2(f(v), f(w)) = \psi_1(v, w) \text{ for all } v, w \in V_1.$$

2.2. Positive definite forms and involutions. In this section we study positivity properties of Hermitian forms on semisimple \mathbb{Q} - and \mathbb{R} -algebras with involution.

We begin by making definitions when $(D, *)$ is a semisimple \mathbb{R} -algebra with involution. Let V be a finite-dimensional right D -module.

We say that a $(D, *)$ -Hermitian form $\psi: V \times V \rightarrow D$ is **positive definite** if

$$\text{Tr}(\psi(v, v); D) > 0 \text{ for all } v \in V - \{0\},$$

where the trace is taken with respect to the action of D on itself (viewed as an \mathbb{R} -vector space) by left multiplication. Note that a skew-Hermitian form can never be positive definite because it will have $\text{Tr}(\psi(v, v); D) = 0$ for all $v \in V$.

We say that a symmetric element $d \in D$ is **positive** if the $(D, *)$ -Hermitian form on D itself given by

$$(v, w) \mapsto v^*dw$$

is positive definite.

We say that $*$ is a **positive involution** if 1 is a positive element of D with respect to $*$. In other words, the bilinear form $(v, w) \mapsto \text{Tr}(v^*w; D): D \times D \rightarrow \mathbb{R}$ is positive definite.

If $(D, *)$ is a semisimple \mathbb{Q} -algebra with involution, then we make the same definitions as above with $\text{Tr}_{D/\mathbb{R}}$ replaced by $\text{Tr}_{D/\mathbb{Q}}$. In other words, an involution of a \mathbb{Q} -algebra D is positive if and only if its extension to $D \otimes_{\mathbb{Q}} \mathbb{R}$ is positive, and similarly for the other definitions.

The lemmas below apply to both semisimple \mathbb{R} -algebras and semisimple \mathbb{Q} -algebras D . For each lemma we either begin by reducing to the case of \mathbb{R} -algebras, or the proof applies directly to both cases.

Lemma 2.2. *If $\psi: V \times V \rightarrow D$ is a positive definite $(D, *)$ -Hermitian form, then the associated adjoint involution $\dagger: \text{End}_D(V) \rightarrow \text{End}_D(V)$ is positive.*

Proof. If the base field is \mathbb{Q} , replace D by $D \otimes_{\mathbb{Q}} \mathbb{R}$. This does not change either the premise or the conclusion of the lemma.

By [Kot92] Lemma 2.2, \dagger is a positive involution if and only if

$$\mathrm{Tr}(xx^\dagger; \mathrm{End}_{\mathbb{R}}(V)) > 0 \quad (2.1)$$

for all $x \in \mathrm{End}_D(V) - \{0\}$, where $\mathrm{End}_D(V)$ acts on $\mathrm{End}_{\mathbb{R}}(V)$ by left multiplication.

Let θ denote the adjoint involution of $\mathrm{End}_{\mathbb{R}}(V)$ with respect to the symmetric \mathbb{R} -bilinear form

$$\mathrm{Tr}(\psi(-, -); D): V \times V \rightarrow \mathbb{R}.$$

Observe that \dagger is the restriction of θ to $\mathrm{End}_D(V)$, so in order to prove (2.1) it suffices to prove that θ is a positive involution of $\mathrm{End}_{\mathbb{R}}(V)$.

All positive definite symmetric bilinear forms on a real vector space are isometric, so we can replace $\mathrm{Tr} \psi$ by the standard symmetric form on \mathbb{R}^n (where $n = \dim_{\mathbb{R}} V$). This replaces θ by the transpose involution of $M_n(\mathbb{R})$, which is well-known to be a positive involution. \square

Lemma 2.3. *If $\psi: V \times V \rightarrow D$ is a positive definite $(D, *)$ -Hermitian form and $q \in \mathrm{End}_D(V)$ is symmetric and positive with respect to the adjoint involution \dagger associated with ψ , then*

$$\psi_q: (v, w) \mapsto \psi(v, qw)$$

*is a positive definite $(D, *)$ -Hermitian form on V .*

Proof. If the base field is \mathbb{Q} , replace D by $D \otimes_{\mathbb{Q}} \mathbb{R}$. This does not change either the premise or the conclusion of the lemma.

The fact that q is symmetric implies that ψ is Hermitian.

By Lemma 2.2, \dagger is a positive involution of $\mathrm{End}_D(V)$. Hence we can apply [Kot92] Lemma 2.8 to obtain $b \in \mathrm{End}_D(V)$ such that $q = bb^\dagger$.

We then have

$$\psi_q(v, v) = \psi(v, bb^\dagger v) = \psi(b^\dagger v, b^\dagger v) > 0$$

for all $v \in V - \{0\}$. \square

Lemma 2.4. *Suppose that D is a division algebra. Let $E = \mathrm{End}_D(V)$ and suppose that we are given a positive involution \dagger of E .*

Then there exist

- (1) *a positive involution $*$ of D , and*
- (2) *a positive definite $(D, *)$ -Hermitian form $\psi: V \times V \rightarrow D$*

such that \dagger is the adjoint involution associated with ψ .

Proof. This proof applies directly to both \mathbb{Q} -algebras and \mathbb{R} -algebras.

The algebras D and E are similar. Hence [KMRT98] Proposition I.3.1 tells us that D possesses an involution $!$ whose restriction to the centre is the same as that of \dagger . By Proposition 2.1, there exists a $(D, !)$ -Hermitian or -skew-Hermitian form $\phi: V \times V \rightarrow D$ such that \dagger is the adjoint involution with respect to ϕ . However, the

involution $!$ might not be positive and ϕ might not be a positive definite Hermitian form.

By Claim 1 below, there is some $v_0 \in V$ such that $\phi(v_0, v_0) \neq 0$. Let

$$s = \phi(v_0, v_0) \in D^\times$$

and observe that $s^! = \epsilon s$, where $\epsilon = +1$ or -1 according as ϕ is $(D, !)$ -Hermitian or $-$ -skew-Hermitian.

Define a new involution $*$ of D and a new bi-additive map $\psi: V \times V \rightarrow D$ by

$$d^* = s^{-1}d^!s$$

and

$$\psi(v, w) = s^{-1}\phi(v, w).$$

Calculations show that ψ is a $(D, *)$ -Hermitian form (regardless of the sign of ϵ) and that \dagger is the associated adjoint involution of E . The facts that $*$ is positive and that ψ is positive definite are Claims 2 and 3 below.

Claim 1. *There exists $v_0 \in V$ such that $\phi(v_0, v_0) \neq 0$.*

Assume for contradiction that $\phi(v, v) = 0$ for all $v \in V$. Since ϕ is non-singular, we can choose $v_1, v_2 \in V$ such that $\phi(v_1, v_2) \neq 0$. By multiplying v_2 by a suitable element of D , we can assume that $\phi(v_1, v_2) = 1$.

Define a D -endomorphism $e: V \rightarrow V$ by

$$e(v) = v_1 \epsilon \phi(v_2, v) - v_2 \phi(v_1, v).$$

A calculation shows that $e^\dagger = -e$. Further calculations (using the assumption that $\phi(v_1, v_1) = \phi(v_2, v_2) = 0$) give

$$ee^\dagger(v_1) = -v_1, \quad ee^\dagger(v_2) = -v_2, \quad ee^\dagger(v) = 0 \text{ if } \phi(v_1, v) = \phi(v_2, v) = 0.$$

It follows that ee^\dagger acts as multiplication by -1 on the right D -module spanned by v_1 and v_2 , and as multiplication by 0 on the right D -module

$$\{v \in V : \psi_0(v_1, v) = \psi_0(v_2, v) = 0\}.$$

These two submodules span V , and so $\text{Tr}(ee^\dagger; V) < 0$. According to [Kot92] Lemma 2.2, this contradicts the positivity of \dagger .

Claim 2. *$\psi: V \times V \rightarrow D$ is positive definite.*

For each $v \in V - \{0\}$, define an endomorphism $e_v \in E$ by

$$e_v(w) = v \psi(v_0, w).$$

By construction, $\psi(v_0, v_0) = s^{-1}s = 1$ and so

$$e_v(v_0) = v.$$

A calculation shows that

$$e_v^\dagger(w) = v_0 \psi(v, w) \text{ for all } w \in V$$

and hence

$$e_v^\dagger e_v(v_0) = v_0 \psi(v, v).$$

Meanwhile, $e_v^\dagger e_v(w) = 0$ if $\psi(v_0, w) = 0$. The submodules $v_0 D$ and

$$\{w \in V : \psi(v_0, w) = 0\}$$

span V and so

$$\mathrm{Tr}(e_v^\dagger e_v; V) = \mathrm{Tr}(\psi(v, v); D).$$

Because \dagger is positive, [Kot92] Lemma 2.2 implies that $\mathrm{Tr}(e_v^\dagger e_v; V) > 0$. Hence we have shown that ψ is positive definite.

Claim 3. ** is a positive involution of D .*

For each $d \in D - \{0\}$, we have

$$d^* d = d^* \psi(v_0, v_0) d = \psi(v_0 d, v_0 d).$$

Hence the fact that ψ is positive definite implies that $*$ is a positive involution. \square

2.3. Lattices and Hermitian forms. Let S_0 be a Dedekind domain and F_0 its field of fractions. Let F be one of the following F_0 -algebras:

- (i) $F = F_0$;
- (ii) F is a separable quadratic extension of F_0 ;
- (iii) $F = F_0 \times F_0$.

Let S be the integral closure of S_0 in F .

Let $x \mapsto \bar{x}$ denote the identity automorphism of F in case (i), and the non-trivial element of $\mathrm{Aut}(F/F_0)$ in cases (ii) and (iii).

Throughout section 2.3, we assume that:

- (a) 2 is invertible in S_0 ; and
- (b) in case (ii), F/F_0 is unramified at all primes of S_0 .

Let V be a finite-dimensional F -module and $\psi: V \times V \rightarrow F$ an F_0 -bilinear form of one of the following types:

- (i) if $F = F_0$, then ψ is either symmetric or skew-symmetric;
- (ii) otherwise, ψ is $(F, \bar{\ })$ -Hermitian.

By a **lattice** in a finite-dimensional F -module V , we mean a finitely generated S -submodule which spans V over F .

The **scale** $\mathfrak{s}\Lambda$ of a lattice Λ (with respect to ψ) is the fractional ideal of F generated by $\psi(\Lambda, \Lambda)$. In paragraph 4.6 of [Shi97], this is denoted $\mu_0(\Lambda)$.

If $F = F_0$ and ψ is symmetric or if $F \neq F_0$, then one can also define the **norm ideal** $\mu(\Lambda)$ to be the fractional ideal of F_0 generated by $\{\psi(v, v) : v \in \Lambda\}$. Our hypotheses that 2 is invertible in S and that F/F_0 is unramified imply that

$$\mathfrak{s}\Lambda = \mu(\Lambda)S_0.$$

It follows that $\mathfrak{s}\Lambda$ and $\mu(\Lambda)$ determine each other, and we are free to use $\mathfrak{s}\Lambda$ in place of $\mu(\Lambda)$ when applying results from [Shi97].

If $F = F_0$ and ψ is skew-symmetric, then the ideal called $\mu(\Lambda)$ in the above paragraph is equal to zero. Hence in this case it only makes sense to consider $\mathfrak{s}\Lambda$, and it is the same as what is called $N(\Lambda)$ in [Shi63].

We say that a lattice Λ is **maximal** with respect to ψ if there is no lattice which strictly contains Λ and which has the same scale as Λ . We say that Λ is **\mathfrak{a} -maximal** if Λ is maximal and $\mathfrak{s}\Lambda = \mathfrak{a}$.

In section 5, we will use the following facts about maximal lattices. In the following lemmas, we assume that F, F_0, S, S_0, V and $\psi: V \times V \rightarrow F$ are as above.

Lemma 2.5. *Let Λ be a lattice in V and let \mathfrak{a} be a fractional ideal of F_0 such that $\mathfrak{s}\Lambda \subset \mathfrak{a}$.*

Then there exists an \mathfrak{a} -maximal lattice in V which contains Λ .

Proof. If $F = F_0$ and ψ is symmetric or if $F \neq F_0$, then this is [Shi97] Lemma 4.8.

If $F = F_0$ and ψ is skew-symmetric, then this is the sentence immediately preceding Proposition 1.4 in [Shi63]. \square

Lemma 2.6. *Let \mathfrak{a} be a fractional ideal of F_0 . All \mathfrak{a} -maximal lattices in V are isometric.*

Proof. If $F = F_0$ and ψ is symmetric or if F/F_0 is a quadratic field extension, then this is [Shi97] Lemma 5.9.

If $F = F_0 \times F_0$, then this is [Shi97] Lemma 4.12.

If $F = F_0$ and ψ is skew-symmetric, then this follows from [Shi63] Proposition 1.4. \square

Lemma 2.7. *Let \dagger be the adjoint involution of $\text{End}_F(V)$ with respect to ψ .*

Let $\Lambda \subset V$ be a lattice and let R be the stabilizer in $\text{End}_F(V)$ of Λ . Suppose that R is a maximal order in $\text{End}_F(V)$ and that \dagger maps R into itself.

Then Λ is a maximal lattice with respect to ψ .

Proof. Let $\mathfrak{a} = \mathfrak{s}\Lambda$ and let

$$\Lambda^* = \{v \in V \mid \psi(v, \Lambda) \subset \mathfrak{a}\}.$$

Observe that any lattice which contains Λ and which has scale \mathfrak{a} must be contained in Λ^* . Hence in order to prove that Λ is maximal, it suffices to show that $\Lambda = \Lambda^*$.

Since R is \dagger -stable, we have

$$\psi(Rv, w) = \psi(v, Rw) \subset \mathfrak{a} \text{ for all } v \in \Lambda^*, w \in \Lambda.$$

Hence R stabilizes Λ^* . Since R is a maximal order in $\text{End}_F(V)$, it follows that R is equal to the stabilizer of Λ^* .

In other words Λ and Λ^* have the same stabilizer, and so $\Lambda^* = u\Lambda$ for some scalar $u \in F^\times$. This implies that

$$\psi(\Lambda^*, \Lambda) = \bar{u}\psi(\Lambda, \Lambda).$$

But the definition of Λ^* implies that $\psi(\Lambda^*, \Lambda) \subset \mathfrak{a}$ so $\bar{u}\mathfrak{a} \subset \mathfrak{a}$. This implies that $\bar{u} \in S$ so also $u \in S$. Hence $\Lambda^* \subset \Lambda$.

The inclusion $\Lambda \subset \Lambda^*$ is obvious. \square

3. AN EXAMPLE OF POLARIZED ISOGENY CLASSES

We give an example to show that polarized isogeny classes truly can be smaller than isogeny classes.

The monoid of polarizations of an abelian variety depends on its endomorphism ring, and hence the same is true for the number of polarized isogeny classes contained in the isogeny class of that abelian variety. If (A, λ) is a principally polarized abelian variety such that $\text{End } A$ is either \mathbb{Z} or an order in an imaginary quadratic field, then all polarizations of A must have the form $n \cdot \lambda$ for some $n \in \mathbb{Z}$. Hence in these cases (which include all elliptic curves over fields of characteristic zero), all isogenies from A to another principally polarized abelian variety are automatically polarized isogenies.

The following proposition shows that this fails when we consider the next simplest case, namely abelian surfaces with multiplication by a real quadratic field.

Proposition 3.1. *Let (A, λ) be a principally polarized abelian variety over an algebraically closed field, such that $\text{End}(A)$ is the ring of integers of a real quadratic field.*

There are infinitely many distinct polarized isogeny classes of principally polarized abelian varieties, all isogenous to A .

Proof. Let $\mathfrak{o}_F = \text{End } A$ and let $F = \mathfrak{o}_F \otimes_{\mathbb{Z}} \mathbb{Q}$.

For each totally positive element $q \in \mathfrak{o}_F$, there is a principally polarized abelian surface (A_q, λ_q) and an isogeny $f_q: A \rightarrow A_q$ such that

$$f_q^* \lambda_q = \lambda \circ q.$$

This can be seen by applying the proof of [Mum70] p. 234 Corollary 1 to A , using a line bundle L associated with the polarisation $\lambda \circ q$.

Suppose that for two totally positive elements q and $r \in \mathfrak{o}_F$, there exists a polarized isogeny $g: A_q \rightarrow A_r$. By definition, we have

$$g^* \lambda_r = n \lambda_q$$

for some $n \in \mathbb{Z}$. Letting $u = f_r^{-1} g f_q \in \text{End } A \otimes_{\mathbb{Z}} \mathbb{Q}$, we find that

$$nq = u^\dagger r u$$

where \dagger is the Rosati involution of $\text{End } A$ induced by λ . In the case we are considering, where the endomorphism algebra is a real quadratic field, the Rosati involution is the identity.

We conclude that (A_q, λ_q) and (A_r, λ_r) are in the same polarized isogeny class if and only if there exist $n \in \mathbb{Z}$ and $u \in \mathfrak{o}_F$ such that

$$nq = u^2 r,$$

or equivalently if and only if

$$q/r \in \mathbb{Q}^\times F^{\times 2}.$$

It follows that $q \mapsto (A_q, \lambda_q)$ is an injection from $F^{+, \times} / \mathbb{Q}^{+, \times} F^{\times 2}$ to the set of polarized isogeny classes of principally polarized abelian varieties isogenous to A , where $F^{+, \times}$ means the multiplicative group of totally positive elements of F .

The group $F^{+, \times} / \mathbb{Q}^{+, \times} F^{\times 2}$ is infinite because there are infinitely many rational primes which split in \mathfrak{o}_F as a product of two principal prime ideals

$$(p) = (a_p)(a'_p).$$

In this splitting, we can always choose a_p totally positive, and the elements $a_p \in \mathfrak{o}_F$ for different p are in different classes in $F^{+, \times} / \mathbb{Q}^{+, \times} F^{\times 2}$. \square

4. POLARIZED ISOGENIES AND FOURTH POWERS OF ABELIAN VARIETIES

In this section we will prove Theorem 1.1, that is, if two principally polarized abelian varieties are isogenous then their fourth powers are in the same polarized isogeny class. The proof uses Theorem 1.2, which asserts that for all positive definite Hermitian forms over a division \mathbb{Q} -algebra with positive involution, the isometry class of the direct sum of four copies of the Hermitian form does not depend on the form we started with.

4.1. Proof that Theorem 1.2 implies Theorem 1.1. Let (A, λ) and (B, μ) be principally polarized abelian varieties and let $f: A \rightarrow B$ be an isogeny. Let $E = \text{End } A \otimes_{\mathbb{Z}} \mathbb{Q}$. Then E is a semisimple \mathbb{Q} -algebra equipped with a positive involution \dagger , the Rosati involution with respect to the polarization λ .

Now $f^* \mu$ is a polarization of A and so there is a symmetric endomorphism $q \in E$ such that

$$f^* \mu = \lambda \circ q. \tag{4.1}$$

Furthermore, q is positive with respect to \dagger . The positivity can be proved by adapting the proof of [Mum70] §21 Theorem 1: if λ and $\lambda \circ q$ are the polarizations associated with the divisors D and D_q respectively, and E^λ and $E^{\lambda q}$ are the associated Riemann forms, then [Mum70] §20 Theorem 3 tells us that for any $a \in \text{End } A$,

$$(E^\lambda)^{\wedge(g-1)} \wedge a^*(E^{\lambda q}) = (D^{g-1} \cdot a^*(D_q)) \cdot v$$

for a suitable generator v of $\text{Hom}_{\mathbb{Z}_\ell}(\wedge^{2g} T_\ell A, \mathbb{Z}_\ell(g))$. Following the proof of [Mum70] §21 Theorem 1 we deduce that

$$\text{Tr}(a^\dagger q a) = \frac{2g}{(D^g)} (D^{g-1} \cdot a^*(D_q)).$$

Because D is ample and $a^*(D_q)$ is effective, this is positive for all $a \in \text{End } A - \{0\}$.

We shall use Theorem 1.2 to prove that there exists $u \in M_4(E)$ such that

$$u^\dagger \text{diag}_4(q) u = 1. \tag{4.2}$$

Once we have obtained such a u , we can clear denominators by finding an integer n such that $nu \in M_4(\text{End } A)$. Thus in $M_4(\text{End } A) = \text{End}(A^4)$, we have

$$(nu)^\dagger \text{diag}_4(q) nu = n^2.$$

We can then carry out the following calculation in $\text{Hom}(A^4, A^{\vee 4})$:

$$\begin{aligned} n^2 \text{diag}_4(\lambda) &= \text{diag}_4(\lambda) (nu)^\dagger \text{diag}_4(q) nu \\ &= (nu)^\vee \text{diag}_4(\lambda) \text{diag}_4(q) nu && \text{(definition of Rosati involution)} \\ &= (nu)^*(\text{diag}_4(\lambda q)) && \text{(definition of } (nu)^*) \\ &= (nu)^*(\text{diag}_4(f^* \mu)) && \text{(by (4.1))} \\ &= (\text{diag}_4(f) \circ nu)^*(\text{diag}_4(\mu)). \end{aligned}$$

Hence $\text{diag}_4(f) \circ nu$ is the desired polarized isogeny $(A, \lambda)^4 \rightarrow (B, \mu)^4$.

To prove that (4.2) has a solution, write E as a direct product of simple \mathbb{Q} -algebras. Because \dagger is a positive involution, it stabilizes each simple factor of E and restricts to a positive involution of the factor. Hence it will suffice to solve (4.2) independently in each factor and combine the solutions.

We therefore restrict to the case in which E is simple i.e. $E = \text{End}_D(V)$ for some division algebra D and some right D -module V . Using Lemma 2.4, choose a positive involution $*$ of D and a positive definite $(D, *)$ -Hermitian form $\psi: V \times V \rightarrow D$ such that \dagger is the associated adjoint involution.

Let $\psi_q: V \times V \rightarrow D$ be defined by

$$\psi_q(v, w) = \psi(v, qw).$$

By Lemma 2.3, this is also a positive definite $(D, *)$ -Hermitian form. So by Theorem 1.2, $\psi_q^{\oplus 4}$ is isometric to $\psi^{\oplus 4}$, or equivalently, there is a solution to (4.2).

4.2. Proof of Theorem 1.2. We are given a division algebra D over \mathbb{Q} with a positive involution $*$ and two positive definite $(D, *)$ -Hermitian forms $\psi_1, \psi_2: V \times V \rightarrow D$. We have to show that $\psi_1^{\oplus 4}$ and $\psi_2^{\oplus 4}$ are isometric.

We split the proof into cases depending on the type of $(D, *)$ in the Albert classification of division algebras with positive involution (see [Mum70] §21 Theorem 2). In each case we use the classification of $(D, *)$ -Hermitian forms from chapter 10 of [Sch85].

Note that $\psi_1^{\oplus 4}$ and $\psi_2^{\oplus 4}$ trivially have the same dimension. They also always have the same signatures at all real places because they are assumed to be positive definite.

Type I. D is a totally real number field and the involution $*$ is trivial, so $(D, *)$ -Hermitian forms are just quadratic forms over D . Isometry classes of quadratic forms over a number field D are classified by their dimension, their determinant in $D^\times/D^{\times 2}$, their Hasse invariant in $\text{Br } D$ and their signatures at real places of D ([Sch85] Corollary 6.6.6).

The determinant of $\psi_1^{\oplus 4}$ is the fourth power of $\det \psi_1$, so is in $D^{\times 2}$, and similarly for $\psi_2^{\oplus 4}$.

It remains to show that the Hasse invariants $s(\psi_1^{\oplus 4})$ and $s(\psi_2^{\oplus 4})$ are the same. We shall prove this by proving that $s(\psi_1^{\oplus 4})$ is the trivial element of $\text{Br } D$; the same proof shows that $s(\psi_2^{\oplus 4})$ is also trivial.

To prove that $s(\psi_1^{\oplus 4})$ is trivial, we will use Lemma 2.12.6 from [Sch85]. This says that

$$s(\phi \oplus \psi) = s(\phi)s(\psi)\sigma(\det \phi, \det \psi)$$

for any quadratic forms ϕ and ψ over D , where $\sigma: D^{\times}/D^{\times 2} \times D^{\times}/D^{\times 2} \rightarrow \text{Br } D$ denotes the Hilbert symbol. In our case, we deduce that

$$s(\psi_1^{\oplus 4}) = s(\psi_1^{\oplus 2})^2 \sigma(\det \psi_1^{\oplus 2}, \det \psi_1^{\oplus 2}).$$

Since s takes values in the 2-torsion subgroup of $\text{Br } D$, $s(\psi_1^{\oplus 2})^2$ is trivial. Since $\det \psi_1^{\oplus 2}$ is a square,

$$\sigma(\det \psi_1^{\oplus 2}, \det \psi_1^{\oplus 2}) = 1.$$

Hence $s(\psi_1^{\oplus 4})$ is trivial.

Type II. D is a totally indefinite quaternion algebra whose centre is a totally real number field F and $*$ is an orthogonal involution.

There is a localization map on the Witt group of $(D, *)$ -Hermitian forms

$$r: W(D, *) \rightarrow \prod_{\mathfrak{p}} W(D_{\mathfrak{p}}, *)$$

where the product on the right hand side runs over all places of F , but this map is not injective. We will first show that $[\psi_1^{\oplus 2}] - [\psi_2^{\oplus 2}]$ is in the kernel of r , then use the fact that $\ker r$ has exponent 2.

For each non-archimedean place \mathfrak{p} of F , we first note that by [Sch85] Remark 7.6.7 the classification of $(D_{\mathfrak{p}}, *)$ -Hermitian forms is equivalent to the classification of $(D_{\mathfrak{p}}, \bar{})$ -skew-Hermitian forms, where $\bar{}$ denotes the canonical involution of $D_{\mathfrak{p}}$.

Hence we can apply [Sch85] Theorem 10.3.6: non-singular $(D_{\mathfrak{p}}, \bar{})$ -skew-Hermitian forms are classified by their dimension and their determinant in $F^{\times}/F^{\times 2}$. The determinants of $\psi_1^{\oplus 2}$ and of $\psi_2^{\oplus 2}$ are both squares, so $\psi_1^{\oplus 2}$ and $\psi_2^{\oplus 2}$ are locally isometric at every non-archimedean place.

At each archimedean place \mathfrak{p} of F , $(D_{\mathfrak{p}}, *) \cong (M_2(\mathbb{R}), \text{transpose})$ so $(D_{\mathfrak{p}}, *)$ -Hermitian forms on $D_{\mathfrak{p}}^n$ are just quadratic forms on \mathbb{R}^{2n} . Hence they are classified by their dimension and signature. Thus $\psi_1^{\oplus 2}$ and $\psi_2^{\oplus 2}$ are locally isometric at archimedean places.

Hence

$$[\psi_1^{\oplus 2}] - [\psi_2^{\oplus 2}] \in \ker r.$$

According to [Lew82] Proposition 3,

$$\ker r \cong (\mathbb{Z}/2\mathbb{Z})^{s-2}$$

where s is the number of places of F at which D is non-split. In fact the statement of [Lew82] Proposition 3 only tells us the order of $\ker r$, not its precise group structure. However the group structure can be deduced from the proof of [Lew82] Proposition 3 or by using the fact that section 4 of [Lew82] exhibits an explicit homomorphism from $\ker r$ into a quotient of $(\mathbb{Z}/2)^s$.

In particular $\ker r$ has exponent 2 and so

$$[\psi_1^{\oplus 4}] - [\psi_2^{\oplus 4}] = 2([\psi_1^{\oplus 2}] - [\psi_2^{\oplus 2}]) = 0$$

in $W(D, *)$. Since $\psi_1^{\oplus 4}$ and $\psi_2^{\oplus 4}$ represent the same element of the Witt group and have the same dimension, they are isometric.

Type III. D is a totally definite quaternion algebra whose centre is a totally real number field F and $*$ is the canonical involution of D .

According to [Sch85] Examples 10.1.8, $(D, *)$ -Hermitian forms are classified by their dimension and signatures at all real places of F . As remarked above, this implies that $\psi_1^{\oplus 4}$ and $\psi_2^{\oplus 4}$ are isometric.

Type IV. D is a division algebra whose centre is a CM field F and $*$ is an involution of the second kind. Let F_0 be the fixed field of $*$ in F .

By [Sch85] Corollary 10.6.6, $(D, *)$ -Hermitian forms are classified by their dimension, their determinant in $F_0^\times / N_{F/F_0}(F^\times)$ and their signatures at all real places of F_0 which do not decompose in F . In our case F is a CM field so all real places of F_0 decompose in F and the signature condition is empty.

The determinants $\det(\psi_1^{\oplus 4})$ and $\det(\psi_2^{\oplus 4})$ are squares in F_0^\times and hence are in $N_{F/F_0}(F^\times)$ as required. So $\psi_1^{\oplus 4}$ and $\psi_2^{\oplus 4}$ are isometric.

This completes the proof of Theorem 1.2.

5. BOUND FOR THE DEGREE OF POLARIZED ISOGENIES

In this section we prove Theorem 1.3 and Proposition 1.5, on the existence of polarized isogenies of polynomially bounded degree. We will begin with a technical definition of norms on semisimple algebras, then explain how Proposition 1.5 implies Theorem 1.3 and give an outline of the proof of Proposition 1.5 before we go through all the details of the latter proof.

5.1. Norms in semisimple algebras. We define a **norm** on a semisimple \mathbb{Q} -algebra E to be a function $N_E: E \rightarrow \mathbb{Q}$ which has the form

$$N_E(x) = \prod_i \left| N_{F_i/\mathbb{Q}}(\text{Nrd}_{E_i/F_i}(x_i)) \right|^{\gamma_i}$$

for some positive integers γ_i , where $E = \prod_i E_i$ as a product of simple algebras and F_i is the centre of E_i . The **rank** of the norm is defined to be the integer d such that

$$N_E(x) = |x|^d \text{ for } x \in \mathbb{Q}.$$

We say that the norm N_E is \dagger -**compatible** if $N_E \circ \dagger = N_E$, where \dagger is an involution of E (in other words, this requires that $\gamma_i = \gamma_j$ whenever \dagger exchanges the simple factors E_i and E_j).

The purpose of this definition is that “degree” is an example of such a norm on the endomorphism algebra of an abelian variety. In particular we have to allow the exponents γ_i to be greater than 1 and to depend on i in order for this to hold for all abelian varieties.

This definition has the following obvious properties:

- (1) $N_E(x) > 0$ for all $x \in E^\times$.
- (2) $N_E(xy) = N_E(x)N_E(y)$ for all $x, y \in E$.
- (3) $N_E(x) \in \mathbb{Z}$ if x is an element of an order in E .
- (4) $N_E(x) = 1$ if x is a unit in an order in E .

Lemma 5.1. *Let E be a semisimple \mathbb{Q} -algebra, $R \subset E$ an order and $N_E: E \rightarrow \mathbb{Q}$ a norm.*

For all $x \in R - \{0\}$, $N_E(x)x^{-1} \in R$.

Proof. Define the reduced characteristic polynomial $P_x(T) \in \mathbb{Q}[T]$ of $x \in E$ as follows. Let $E = \prod_i E_i$ as a product of simple algebras, and let F_i be the centre of E_i . Let $Q_{x,i}(T)$ be the characteristic polynomial over \mathbb{Q} of x_i acting on E_i by left multiplication. If $\dim_{F_i} E_i = n_i^2$, then $Q_{x,i}(T) = P_{x,i}(T)^{n_i}$ for some polynomial $P_{x,i}(T) \in \mathbb{Q}[T]$. We define

$$P_x(T) = \prod_i P_{x,i}(T).$$

Label the coefficients of P_x as

$$P_x(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0.$$

Since $P_x(x) = 0$, we get

$$-a_0x^{-1} = x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1. \quad (5.1)$$

Since $x \in R$, the coefficients of P_x are all in \mathbb{Z} . Hence the right hand side of (5.1) is in R . We deduce that $a_0x^{-1} \in R$.

The definition of reduced norms implies that

$$a_0 = \pm \prod_i N_{F_i/\mathbb{Q}}(\text{Nrd}_{E_i/F_i}(x_i)).$$

Since $N_{F_i/\mathbb{Q}}(\text{Nrd}_{E_i/F_i}(x_i)) \in \mathbb{Z}$ and $\gamma_i \geq 1$ for all i , we deduce that

$$N_E(x)a_0^{-1} = \pm \prod_i N_{F_i/\mathbb{Q}}(\text{Nrd}_{E_i/F_i}(x_i))^{\gamma_i-1}$$

is an integer.

We conclude that

$$N_E(x)x^{-1} = (N_E(x)a_0^{-1})(a_0x^{-1}) \in R. \quad \square$$

We also make a local analogue of the above definition of norms. We define a **norm** on a semisimple \mathbb{Q}_p -algebra E_p to be a function $N_{E_p}: E_p \rightarrow \mathbb{Q}$ of the form

$$N_{E_p}(x) = \prod_i \left| N_{F_i/\mathbb{Q}_p}(\text{Nrd}_{E_i/F_i}(x_i)) \right|_p^{-\gamma_i}$$

for some positive integers γ_i , where $E = \prod_i E_i$ as a product of simple algebras and F_i is the centre of E_i . The **rank** of N_{E_p} is defined to be the positive integer d such that

$$N_{E_p}(x) = |x|_p^{-d} \text{ for all } x \in \mathbb{Q}_p.$$

Note that the exponents in the definition of a local norm are negative. This is because $|x|_p \leq 1$ when x is a p -adic integer, and so local norms N_{E_p} satisfy property (3) above. Indeed, it is simple to check that all of properties (1)–(4) above and Lemma 5.1 hold for a local norm N_{E_p} .

Furthermore, if N_E is a norm on a semisimple \mathbb{Q} -algebra E , then the extensions of N_E to the localizations $E \otimes_{\mathbb{Q}} \mathbb{Q}_p$ satisfy

$$N_E(x) = \prod_p N_{E \otimes_{\mathbb{Q}} \mathbb{Q}_p}(x) \text{ for all } x \in E.$$

5.2. Proof that Proposition 1.5 implies Theorem 1.3. We are given principally polarized abelian varieties (A, λ) and (B, μ) and isogenies $f, g: A \rightarrow B$ such that f is a polarized isogeny and $\deg g = n$. We want to prove the existence of a polarized isogeny $h: A \rightarrow B$ of degree at most cn^k , where c and k depend only on (A, λ) .

We will apply Proposition 1.5 to $R = \text{End } A$ and $E = R \otimes_{\mathbb{Z}} \mathbb{Q}$, with \dagger being the Rosati involution with respect to the polarization λ . The norm is given by $N_E(a) = \deg a$ for $a \in \text{End } A$ (this is defined to be 0 if a is not an isogeny), extended homogeneously to E i.e.

$$N_E(a) = \deg(na)/n^{2 \dim A} \text{ where } n \text{ is a non-zero integer such that } na \in \text{End } A.$$

By [Mil86] Proposition 12.12, this is a norm on E as defined above, with degree $2 \dim A$.

Set

$$a = g^{-1}f \in \text{End } A \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Let q be an element of $\text{End } A$ such that $g^*\mu = \lambda \circ q$. A calculation shows that

$$\lambda a^\dagger qa = a^\vee \lambda qa = a^*(\lambda q) = a^*(g^*\mu) = (ga)^*(\mu) = f^*\mu.$$

Hence the fact that f is a polarized isogeny implies that

$$a^\dagger qa \in \mathbb{Q}^\times.$$

We can therefore apply Proposition 1.5 to obtain $b \in \text{End } A$ such that

$$b^\dagger qb \in \mathbb{Z} - \{0\} \text{ and } N_E(b) \leq c N_E(q)^{d-1/2}.$$

The fact that $b^\dagger qb \in \mathbb{Z} - \{0\}$ implies that $h = g \circ b$ is a polarized isogeny $A \rightarrow B$.

The definition of q implies that

$$N_E(q) = (\deg g)^2 = n^2$$

and so the bound from Proposition 1.5 gives

$$\deg h = n N_E(b) \leq cn N_E(q)^{d-1/2} = cn(n^2)^{d-1/2} = cn^{2d}$$

where $d = 2 \dim A$.

5.3. Outline of the proof of Proposition 1.5. Before we come to the proof of Proposition 1.5 in general, we will first look at the case where E is a number field and R is its ring of integers. We will sketch a proof that in this case, there is some $b \in R$ satisfying $b^\dagger qb \in \mathbb{Z} - \{0\}$ and whose norm is bounded by some polynomial in $N_E(q)$, but we will not seek to optimize the bound. Indeed this sketch will give a weaker exponent than is stated in Proposition 1.5.

We begin by looking for an ideal instead of an element of R which satisfies the conclusion of Proposition 1.5. In other words, we look for an ideal $\mathfrak{b} \subset R$ which has suitably bounded norm and which satisfies

$$\mathfrak{b}^\dagger q \mathfrak{b} = mR \text{ for some } m \in \mathbb{Z}. \quad (5.2)$$

Take a as in the hypothesis of Proposition 1.5. Multiplying it by a rational integer, we may assume without loss of generality that $a \in R$. Then the principal ideal aR satisfies (5.2), showing that the set of ideals \mathfrak{b} which satisfy (5.2) is non-empty.

In order to find a solution to (5.2) with small norm, we work locally in $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for each rational prime p , looking at ideals $\mathfrak{b}_p \subset R_p$ which satisfy

$$\mathfrak{b}_p^\dagger q \mathfrak{b}_p = mR_p \text{ for some } m \in \mathbb{Z}_p. \quad (5.3)$$

If qR is coprime to pR , then clearly $\mathfrak{b}_p = R_p$ satisfies (5.3). So we only need to consider the finitely many primes p for which pR is not coprime to qR .

Denote the factorizations into prime ideals in R_p of pR_p and of qR_p by

$$pR_p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \text{ and } qR_p = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}.$$

Given an ideal $\mathfrak{b}_p \subset R_p$ satisfying (5.3), let its prime factorization be

$$\mathfrak{b}_p = \mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_r^{\beta_r}.$$

If p divides \mathfrak{b}_p , then we can replace \mathfrak{b}_p by $p^{-1}\mathfrak{b}_p$ and it will still be an ideal of R_p satisfying (5.3). Hence we can assume that p does not divide \mathfrak{b}_p . This implies that $\beta_i < e_i$ for some i .

Suppose that $\mathfrak{b}_p^\dagger q \mathfrak{b}_p = p^t R_p$. Then

$$t = (2\beta_i + k_i)/e_i \text{ for all } i.$$

Applying this for an i at which $\beta_i < e_i$, we get

$$t < 2 + \max(k_1, \dots, k_r) \leq 2 + v_p(N(qR_p)).$$

A calculation then shows that

$$N(\mathfrak{b}_p) < p^d N(qR_p)^{(d-1)/2}$$

where $d = [E : \mathbb{Q}]$. Since we are assuming that qR is not coprime to pR , $N(qR_p) \geq p$ and so this implies

$$N(\mathfrak{b}_p) < N(qR_p)^{(3d-1)/2}.$$

Letting \mathfrak{b} be the product of the ideals $\mathfrak{b}_p \cap R$, we get an ideal of R which satisfies (5.2) and such that

$$N(\mathfrak{b}) \leq |N_E(q)|^{(3d-1)/2}.$$

Using finiteness of the class group, we may replace the ideal \mathfrak{b} by a principal ideal at the cost of a constant factor in the norm bound. Thus there are $b \in R$, $u \in R^\times$ and $m \in \mathbb{Z}$ such that

$$b^\dagger qb = um.$$

Using the fact that R^\times is finitely generated, we can remove the unit u at the cost of another constant factor.

The argument sketched above relies on E being a field. When E is not a field, our proof will have the same local-global structure, but we will work with adèles instead of ideals. We will begin by proving a local version of Proposition 1.5 for all primes p , namely Lemma 5.3. However, this local version, with a constant c_p for each prime p , is not sufficient to deduce a global result: we need to know that the constants c_p are 1 for almost all p . This is given by Corollary 5.6. Once we have these two local results, we will then use the adelic version of finiteness of the class group to obtain Proposition 1.5.

The local results Lemma 5.3 and Corollary 5.6 are results about lattices and Hermitian forms over division algebras over local fields. (In the commutative case sketched above, the relevant hermitian forms are on 1-dimensional vector spaces, and so can simply be described by scalars.)

In the case of Lemma 5.3, our proof does not use hermitian forms explicitly. However it uses the p -adic polar decomposition of Benoist and Oh [BO07], which can be seen as a generalization of the diagonalization of quadratic forms over a field.

In the proof of Corollary 5.6, we work directly with Hermitian forms. This corollary applies only to primes at which E_p is split, so we only need to consider Hermitian forms over a field instead of over a division algebra. We get the necessary integrality ingredients by using properties of maximal lattices.

5.4. Local calculations – non-split case. We will prove the local version of Proposition 1.5, valid for all primes p but with a non-trivial constant c_p for every prime p . The exponent $(d-1)/2$ in this local result (Lemma 5.3) is better than the $d-1/2$ of Proposition 1.5 but this is not important – the weaker exponent

in Proposition 1.5 comes from Corollary 5.6. Our primary ingredient is the p -adic polar decomposition of Benoist and Oh ([BO07] Theorem 1.1), applied to the element a such that $a^\dagger qa \in \mathbb{Q}_p^\times$.

Here is an outline of the proof of Lemma 5.3. We rearrange the hypothesis $a^\dagger qa \in \mathbb{Q}_p^\times$ to obtain $q^{-1} \in \mathbb{Q}_p^\times aa^\dagger$. The p -adic polar decomposition allows us to write $a = ksh$ where s is fixed by \dagger and is in one of a fixed finite collection of commutative subalgebras of E_p . We can easily deal with k and h , so that instead of aa^\dagger we have to look at s^2 . (In the case where E_p is a matrix algebra over a field and \dagger is the transpose involution, replacing aa^\dagger by s^2 corresponds to diagonalizing the quadratic form with matrix aa^\dagger .)

Some calculations allow us to construct a \mathbb{Q}_p -multiple us of s such that $(us)^2$ is in the order R_p and has bounded norm. The fact that s is in one of a fixed set of commutative subalgebras of E allows us to deduce that a bounded multiple of us is in R_p . Reversing the calculations finishes the proof.

We will need the following lemma once we know that us is in a fixed commutative subalgebra and that $(us)^2$ is in R_p . The key point in the proof of Lemma 5.2 is that the (unique) maximal order in a commutative algebra is integrally closed.

Lemma 5.2. *Let E_p be a semisimple \mathbb{Q}_p -algebra and $R_p \subset E_p$ an order. Let $L \subset E_p$ be a commutative \mathbb{Q}_p -subalgebra.*

There is a positive rational integer c depending on E_p , R_p and L such that: for all $x \in L$, if $x^2 \in R_p$ then $cx \in R_p$.

Proof. Let \mathfrak{o}_L denote the maximal order in L .

$R_p \cap L$ is a \mathbb{Z}_p -subalgebra of L which is finitely generated as a \mathbb{Z}_p -module, so it is contained in \mathfrak{o}_L . $R_p \cap L$ is also open in L (because R_p is open in E_p), so it has finite index in \mathfrak{o}_L . Hence there is $c \in \mathbb{N}$ such that

$$c\mathfrak{o}_L \subset R_p \cap L.$$

Now if $x \in L$ and $x^2 \in R_p$, then $x^2 \in \mathfrak{o}_L$. Since \mathfrak{o}_L is integrally closed, it follows that $x \in \mathfrak{o}_L$ and so $cx \in R_p \cap L$. \square

Let us recall the p -adic polar decomposition of Benoist and Oh. Note that we use a different definition of involution of a group from [BO07]: for us, an involution reverses the order of multiplication, while in [BO07] an involution preserves the order of multiplication. Hence $\dagger: G \rightarrow G$ is an involution in our sense if and only if $g \mapsto (g^\dagger)^{-1}$ is an involution in the sense of [BO07]. This leads to the cosmetic differences between the definitions of \mathbf{H} and of (\mathbb{Q}_p, \dagger) -split tori given below and those in [BO07].

Let \mathbf{G} be a connected reductive algebraic group over \mathbb{Q}_p , let \dagger be an involution of \mathbf{G} , and let \mathbf{H} be the algebraic subgroup

$$\mathbf{H} = \{h \in \mathbf{G} \mid hh^\dagger = 1\}.$$

We say that a torus $\mathbf{S} \subset \mathbf{G}$ is (\mathbb{Q}_p, \dagger) -**split** if \mathbf{S} is split over \mathbb{Q}_p and $s^\dagger = s$ for all $s \in S$. By a theorem of Helminck and Wang [HW93] there are finitely many $\mathbf{H}(\mathbb{Q}_p)$ -conjugacy classes of maximal (\mathbb{Q}_p, \dagger) -split tori in \mathbf{G} . Choose representatives \mathbf{S}_i for these $\mathbf{H}(\mathbb{Q}_p)$ -conjugacy classes of maximal (\mathbb{Q}_p, \dagger) -split tori.

Theorem 1.1 of [BO07] asserts that there exists a compact subset $K \subset \mathbf{G}(\mathbb{Q}_p)$ such that

$$\mathbf{G}(\mathbb{Q}_p) = K \left(\bigcup_i \mathbf{S}_i(\mathbb{Q}_p) \right) \mathbf{H}(\mathbb{Q}_p). \quad (5.4)$$

Lemma 5.3. *Let (E_p, \dagger) be a semisimple \mathbb{Q}_p -algebra with involution, $R_p \subset E_p$ a \dagger -stable order, and N_{E_p} a \dagger -compatible norm on E_p of rank d .*

There exists a constant c_p depending only on (R_p, \dagger, N_{E_p}) such that:

For every $q \in R_p$, if there exists $a \in E_p$ such that $a^\dagger q a \in \mathbb{Q}_p^\times$, then there exists $b \in R_p$ such that

$$b^\dagger q b \in \mathbb{Z}_p - \{0\} \text{ and } N_{E_p}(b) \leq c_p N_{E_p}(q)^{(d-1)/2}.$$

Proof. Let \mathbf{G} be the reductive \mathbb{Q}_p -algebraic group with functor of points

$$\mathbf{G}(A) = (E_p \otimes_{\mathbb{Q}_p} A)^\times.$$

The involution \dagger of E_p induces an involution of \mathbf{G} . Let \mathbf{H} be the subgroup of \dagger -unitary elements and let \mathbf{S}_i be representatives for the $\mathbf{H}(\mathbb{Q}_p)$ -conjugacy classes of maximal (\mathbb{Q}_p, \dagger) -split tori in \mathbf{G} , as above.

Choose a compact subset $K \subset \mathbf{G}(\mathbb{Q}_p)$ satisfying (5.4). Because K is compact, its elements have bounded denominators. Hence after replacing K by a scalar multiple, we may assume that $K \subset R_p$. Since K^{-1} is also compact, we can choose a constant $c_{p,1} \in \mathbb{N}$ such that $c_{p,1} K^{-1} \subset R_p$.

Let $m = a^\dagger q a$. Because m is invertible and in the centre of E_p , we can rearrange this to get

$$q^{-1} = m^{-1} a a^\dagger. \quad (5.5)$$

Let $n = N_{E_p}(q)$. By Lemma 5.1, $nq^{-1} \in R_p$. So (5.5) implies that

$$n m^{-1} a a^\dagger \in R_p.$$

Using the p -adic polar decomposition, write

$$a = k s h$$

with $k \in K$, $s \in \bigcup_i \mathbf{S}_i(\mathbb{Q}_p)$ and $h \in \mathbf{H}(\mathbb{Q}_p)$. Substituting this in the previous equation, and using the facts that $h h^\dagger = 1$ and $s = s^\dagger$, we get that

$$n m^{-1} k s^2 k^\dagger \in R_p.$$

Multiplying by $c_{p,1} k^{-1}$ on the left and $c_{p,1} (k^{-1})^\dagger$ on the right, we get that

$$c_{p,1}^2 n m^{-1} s^2 \in R_p.$$

Choose $e \in \mathbb{Z}_p$ such that $c_{p,1}^2 nm^{-1}e$ is a square in \mathbb{Q}_p^\times and $v_p(e) = 0$ or 1 . Let u denote a square root in \mathbb{Q}_p^\times of $c_{p,1}^2 nm^{-1}e$. We get that

$$u^2 s^2 \in R_p.$$

Furthermore, $us \in \bigcup_i \mathbf{S}_i(\mathbb{Q}_p)$ because the scalars \mathbb{Q}_p^\times are contained in every maximal (\mathbb{Q}_p, \dagger) -split torus of \mathbf{G} . For each i , the subalgebra $L_i \subset E_p$ generated by $\mathbf{S}_i(\mathbb{Q}_p)$ is commutative. We can therefore apply Lemma 5.2 inside each L_i . We deduce that there is a constant $c_{p,2}$ (depending on R_p and the \mathbf{S}_i) such that

$$c_{p,2}us \in R_p.$$

Letting

$$b = c_{p,2}u ks,$$

we get that $b \in R_p$ and

$$bb^\dagger = c_{p,2}^2 u^2 ks^2 k^\dagger = c_{p,1}^2 c_{p,2}^2 nm^{-1} e aa^\dagger = c_{p,1}^2 c_{p,2}^2 ne q^{-1}$$

where the last equality follows from (5.5). Since $c_{p,1}^2 c_{p,2}^2 ne$ is in the centre of E_p , we can rearrange this to obtain

$$b^\dagger qb = c_{p,1}^2 c_{p,2}^2 ne \in \mathbb{Z}_p - \{0\}.$$

Finally we bound the norm of b . The above equation gives us that

$$n N_{E_p}(b)^2 = N_{E_p}(c_{p,1}^2 c_{p,2}^2 ne) = c_{p,1}^{2d} c_{p,2}^{2d} n^d N_{E_p}(e).$$

Since $v_p(e) = 0$ or 1 , $N_{E_p}(e) \leq p^d$. Hence

$$N_{E_p}(b)^2 \leq c_{p,1}^{2d} c_{p,2}^{2d} p^d n^{d-1}.$$

So the lemma is proved with constant $c_p = (c_{p,1}^{2d} c_{p,2}^{2d} p^d)^{1/2}$. \square

5.5. Local calculations – split case. Our goal now is to prove that for all but finitely many primes p , Lemma 5.3 holds with $c_p = 1$. Specifically we will prove this for all p such that E_p is split (meaning that E_p is a product of matrix algebras over fields), the centre of E_p is a product of unramified extensions of \mathbb{Q}_p , R_p is a maximal order in E_p and $p \neq 2$.

The first step in this proof applies to simple algebras with involution (Lemma 5.4). We will then obtain a result for a semisimple algebra with involution (Corollary 5.6) by applying Lemma 5.4 to each of its simple factors. In order to do this, it is not enough just to show that, for each simple factor, there exists some b such that $b^\dagger qb \in \mathbb{Z}_p - \{0\}$. In order that the solutions for different simple factors combine together, it is necessary that the scalars $b^\dagger qb$ should be the same in each factor. Therefore we state Lemma 5.4 in a form which allows to choose the $m' \in \mathbb{Z}_p - \{0\}$ for which we want to solve $b^\dagger qb = m'$, subject to certain constraints.

The statement of Lemma 5.4 does not mention norms at all. The norm bound comes from the choice of m' , which will be made in the proof of Corollary 5.6. The naïve choice for m' leads to a bound

$$N_{E_p}(b) \leq p^{d/2} N_{E_p}(q)^{(d-1)/2}.$$

If $q \notin R_p^\times$, then $N_{E_p}(q) \geq p$ and so we can remove the power of p from the above bound, at the cost of weakening the exponent. On the other hand if $q \in R_p^\times$, then $N_{E_p}(q) = 1$ and we have to have $m' \in \mathbb{Z}_p^\times$ in order to get the desired bound from Lemma 5.4. In order to achieve this, we will need an additional result on the classification of unimodular Hermitian forms (Lemma 5.5).

Lemma 5.4. *Let (E_p, \dagger) be a simple \mathbb{Q}_p -algebra with involution and $R_p \subset E_p$ a \dagger -stable order. Suppose that E_p is split, its centre is an unramified extension of \mathbb{Q}_p , R_p is a maximal order in E_p and $p \neq 2$.*

Let $q \in R_p$ and $a \in E_p$ be such that $a^\dagger qa \in \mathbb{Q}_p^\times$.

Let $m = a^\dagger qa$ and let $m' \in \mathbb{Z}_p - \{0\}$ be such that $m'q^{-1} \in R_p$ and $m'm^{-1}$ is a square in \mathbb{Q}_p^\times .

Then there exists $b \in R_p$ such that

$$b^\dagger qb = m'.$$

Proof. Let F be the centre of E_p and F_0 the subfield of F fixed by \dagger . Since E_p is split, it is isomorphic to $\text{End}_F(V)$ for some F -module V . By Proposition 2.1, there is an F_0 -bilinear form $\psi: V \times V \rightarrow F$ such that \dagger is the adjoint involution with respect to ψ , and we are in the setting of section 2.3.

Since R_p is a maximal order in E_p , we can find a lattice $\Lambda \subset V$ whose stabilizer is R_p . Since R_p is \dagger -stable, Lemma 2.7 implies that Λ is a maximal lattice with respect to ψ . Let \mathfrak{a} be the scale of Λ with respect to ψ .

Let ψ_q be the F_0 -bilinear form $V \times V \rightarrow F$ given by

$$\psi_q(v, w) = \psi(v, qw).$$

A calculation shows that

$$\{v \in V \mid \psi_q(v, m'q^{-1}\Lambda) \subset m'\mathfrak{a}\} = \{v \in V \mid \psi(v, \Lambda) \subset \mathfrak{a}\} = \Lambda \quad (5.6)$$

where the second equality holds because Λ is \mathfrak{a} -maximal (see the proof of Lemma 2.7). Since $m'q^{-1} \in R_p$, we have $m'q^{-1}\Lambda \subset \Lambda$ and hence (5.6) implies that

$$\psi_q(m'q^{-1}\Lambda, m'q^{-1}\Lambda) \subset m'\mathfrak{a}.$$

Hence by Lemma 2.5, there exists a lattice Λ' which is $m'\mathfrak{a}$ -maximal with respect to ψ_q and which contains $m'q^{-1}\Lambda$. Note that Λ' must be contained in

$$\{v \in V \mid \psi_q(v, m'q^{-1}\Lambda) \subset m'\mathfrak{a}\}$$

and so by (5.6), $\Lambda' \subset \Lambda$.

The fact that $m = a^\dagger qa$ implies that $a\Lambda$ is an $m\mathfrak{a}$ -maximal lattice with respect to ψ_q . Choosing a square root $u \in \mathbb{Q}_p^\times$ of $m^{-1}m'$, we deduce that $ua\Lambda$ is an $m'\mathfrak{a}$ -maximal lattice with respect to ψ_q .

Hence by Lemma 2.6, $(ua\Lambda, \psi_q)$ is isometric to (Λ', ψ_q) . It follows that there exists $b \in E_p$ such that

$$\Lambda' = b\Lambda \text{ and } b^\dagger qb = (ua)^\dagger qua.$$

The fact that $\Lambda' \subset \Lambda$ implies that $b \in R_p$, while a calculation gives

$$b^\dagger qb = (ua)^\dagger qua = u^2 a^\dagger qa = u^2 m = m'. \quad \square$$

When $q \in R_p^\times$, we will use the following lemma to enable us to choose an $m' \in \mathbb{Z}_p^\times$ for use in Lemma 5.4. In case (i) we can choose $m' \in \mathbb{Z}_p^\times$ such that $m'(a^\dagger qa)^{-1}$ is a square. In case (ii) we will let $m' = 1$ and apply Lemma 5.4 to b coming from Lemma 5.5 instead of the original a .

Lemma 5.5. *Let (E_p, \dagger) be a simple \mathbb{Q}_p -algebra with involution and $R_p \subset E_p$ a \dagger -stable order. Suppose that E_p is split, its centre is an unramified extension of \mathbb{Q}_p , R_p is a maximal order in E_p and $p \neq 2$.*

Let $q \in R_p$ and $a \in E_p$ be such that $a^\dagger qa \in \mathbb{Q}_p^\times$. Suppose further that $q \in R_p^\times$.

Then either:

- (i) $v_p(a^\dagger qa)$ is even; or*
- (ii) there exists $b \in E_p^\times$ such that $b^\dagger qb = 1$.*

Proof. We use the same notation F, F_0, V, ψ, ψ_q as in the proof of Lemma 5.4.

The hypothesis that $a^\dagger qa \in \mathbb{Q}_p^\times$ tells us that (V, ψ_q) is isometric to $(V, m\psi)$ for the scalar $m = a^\dagger qa \in \mathbb{Q}_p^\times$. In order to show that there exists $b \in E_p^\times$ such that $b^\dagger qb = 1$, we have to show that in fact (V, ψ_q) is isometric to (V, ψ) . There is one case in which it is not true that (V, ψ_q) is isometric to (V, ψ) ; in this case we will show instead that $v_p(m)$ is even, leading to the two cases in the conclusion of the lemma.

We proceed in cases according to the type of the form ψ .

- (1) $F = F_0$ and ψ is symmetric.

Choose a basis for V as an F -vector space, inducing an isomorphism $E_p \cong M_n(F)$. Since R_p is a maximal order in E_p , we can choose the basis such that R_p corresponds to $M_n(\mathfrak{o}_F)$.

We can write the quadratic form ψ in the form

$$\psi(v, w) = v^t z w$$

for some symmetric matrix $z \in M_n(F)$. Then the adjoint involution is given by

$$x^\dagger = z^{-1} x^t z.$$

Since R_p is \dagger -stable, this implies that z normalizes R_p . The normalizer of R_p is $F^\times R_p^\times$, so after multiplying ψ by a scalar in F^\times (which does not

change the defining property of ψ , namely that its adjoint involution is \dagger), we may assume that $z \in R_p^\times = \mathrm{GL}_n(\mathfrak{o}_F)$ and so ψ is a unimodular quadratic form.

Since $q \in R_p^\times$, this implies that $zq \in R_p^\times$ and hence ψ_q is also unimodular. Since $p \neq 2$, [O'M63] 92:1 implies that unimodular quadratic forms over \mathfrak{o}_F are classified by their dimension and their determinant in $F^\times/F^{\times 2}$.

The fact that (V, ψ_q) and $(V, m\psi)$ are isometric implies that

$$\det(\psi_q) = \det(m\psi) = m^n \det(\psi) \text{ in } F^\times/F^{\times 2}. \quad (5.7)$$

If n is even, then (5.7) tells us at once that $\det(\psi_q) = \det(\psi)$ in $F^\times/F^{\times 2}$ and so (V, ψ_q) is isometric to (V, ψ) .

If n is odd, then (5.7) implies that

$$\det(\psi_q) = m \det(\psi) \text{ in } F^\times/F^{\times 2}.$$

Since ψ_q and ψ are both unimodular, we deduce that

$$m \in \mathfrak{o}_F^\times F^{\times 2}.$$

Since F/\mathbb{Q}_p is unramified, this implies that $v_p(m)$ is even.

- (2) $F = F_0$ and ψ is skew-symmetric.

Isometry classes of skew-symmetric forms over a field are classified by their dimension alone, so (V, ψ) and (V, ψ_q) are isometric.

- (3) F/F_0 is a quadratic extension of fields and ψ is Hermitian.

For local fields F and F_0 , isometry classes of non-singular F/F_0 -Hermitian forms are classified by their dimension and their determinant in $F_0^\times/\mathrm{N}_{F/F_0}(F^\times)$ (see [Sch85] Examples 10.1.6(ii)).

Since ψ and ψ_q are both unimodular, $\det \psi$ and $\det \psi_q$ are both in $\mathfrak{o}_{F_0}^\times$. Since the extension F/F_0 is unramified, $\mathrm{N}_{F/F_0}(F^\times)$ contains $\mathfrak{o}_{F_0}^\times$. Hence (V, ψ) and (V, ψ_q) are isometric.

- (4) $F = F_0 \times F_0$ and ψ is Hermitian.

By [Sch85] Example 7.2.7, all non-singular $(F_0 \times F_0)/F_0$ -Hermitian forms of the same dimension are isometric, in particular (V, ψ) and (V, ψ_q) . \square

Corollary 5.6. *Let (E_p, \dagger) be a semisimple \mathbb{Q}_p -algebra with involution, $R_p \subset E_p$ a \dagger -stable order, and N_{E_p} a \dagger -compatible norm on E_p of rank d . Suppose that E_p is split, its centre is a product of unramified extensions of \mathbb{Q}_p , R_p is a maximal order in E_p and $p \neq 2$.*

For every $q \in R_p$, if there exists $a \in E_p$ such that $a^\dagger qa \in \mathbb{Q}_p^\times$, then there exists $b \in R_p$ such that

$$b^\dagger qb \in \mathbb{Z}_p - \{0\} \text{ and } \mathrm{N}_{E_p}(b) \leq \mathrm{N}_{E_p}(q)^{d-1/2}.$$

Proof. Write the algebra E_p as a direct product

$$E_p = \prod_i E_i$$

where each E_i is a simple algebra with involution. Since R_p is a maximal order in E_p , it is a direct product of maximal orders $R_i \subset E_i$.

Let $m = a^\dagger q a$ and $n = N_{E_p}(q)$.

We have two cases, depending on whether $q \in R_p^\times$ or not.

Case 1. If $q \in R_p^\times$, then we apply Lemma 5.5 to each factor E_i . If conclusion (i) of Lemma 5.5 holds for at least one factor E_i , then we know that $v_p(m)$ is even. We can therefore choose some $m' \in \mathbb{Z}_p^\times$ such that $m'm^{-1}$ is a square in \mathbb{Q}_p^\times . Since $q \in R_p^\times$, $m'q^{-1} \in R_p$ and so we can apply Lemma 5.4 in each factor E_i to q_i , a_i and m' to obtain $b_i \in R_i$ such that $b_i^\dagger q_i b_i = m'$.

Otherwise (still within the case $q \in R_p^\times$), conclusion (ii) of Lemma 5.5 holds in every factor E_i . In other words, for each i , there exists $b_i \in E_i^\times$ such that $b_i^\dagger q_i b_i = 1$. In this case, simply let $m' = 1$. Lemma 5.4 allows us to upgrade $b_i \in E_i$ to $b_i \in R_i$.

Letting b be the element of R_p whose components are the b_i , we get that

$$bqb^\dagger = m' \in \mathbb{Z}_p - \{0\}.$$

The fact that $m' \in \mathbb{Z}_p^\times$ implies that $b \in R_p^\times$ and so

$$N_{E_p}(b) = 1 = N_{E_p}(q)^{d-1/2}.$$

Case 2. If $q \notin R_p^\times$, choose $e \in \mathbb{Z}_p$ such that $v_p(e) = 0$ or 1 and nem^{-1} is a square in \mathbb{Q}_p^\times . By Lemma 5.1, $neq^{-1} \in R_p$. So in each factor E_i , we can apply Lemma 5.4 to q_i and a_i with $m' = ne$.

The resulting b_i fit together to give $b \in R_p$ such that

$$b^\dagger qb = ne \in \mathbb{Z}_p - \{0\}.$$

This implies that

$$N_{E_p}(b)^2 N_{E_p}(q) = N_{E_p}(ne) \leq n^d p^d$$

and hence

$$N_{E_p}(b) \leq n^{(d-1)/2} p^{d/2}.$$

Since $q \notin R_p^\times$, we have $p \leq n$ so this implies that $N_{E_p}(b) \leq n^{d-1/2}$. \square

5.6. Global arguments. We are now ready to complete the proof of Proposition 1.5, deducing it from Lemma 5.3 and Corollary 5.6.

We are given a semisimple \mathbb{Q} -algebra E with involution \dagger and a \dagger -stable order $R \subset E$. We will work in the adelic points of the group \mathbf{U} of \dagger -quasi-unitary elements of R , that is, the \mathbb{Z} -group scheme with functor of points

$$\mathbf{U}(A) = \{u \in (R \otimes_{\mathbb{Z}} A)^\times \mid uu^\dagger \in A^\times\}.$$

We are given $q \in R$ and $a \in E$ such that $a^\dagger qa \in \mathbb{Q}^\times$. Our first step is to choose $b_p \in R_p$ for each p such that $b_p^\dagger qb_p \in \mathbb{Q}_p^\times$, and the norms of b_p are bounded according to Lemma 5.3 and Corollary 5.6. We then look at

$$u_p = b_p^{-1}a.$$

Some calculations show that the u_p are components of an adelic element $\mathbf{u} \in \mathbf{U}(\mathbb{A}_f)$.

Finiteness of the adelic class set of \mathbf{U} allows us to write \mathbf{u} as a product of an element x of $\mathbf{U}(\mathbb{Q})$, an element \mathbf{g}_i from a fixed finite set, and an element \mathbf{y} of $\mathbf{U}(\mathbb{A}_f)$ which is a unit at every prime. Then

$$b = ax^{-1}$$

is an element of E which satisfies $b^\dagger qb \in \mathbb{Z} - \{0\}$. Another calculation shows that the norm of b is not far away from $\prod_p N_{E_p}(b_p)$, and hence satisfies the required bound.

Proof of Proposition 1.5. By hypothesis, we have $q \in R$ and $a \in E$ such that

$$a^\dagger qa \in \mathbb{Q}^\times.$$

Let $m = a^\dagger qa$. Since m is in the centre of E , we can deduce that $mq^{-1} = aa^\dagger$.

Applying Lemma 5.3 in each localization $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$, we get $b_p \in R_p$ such that

$$b_p^\dagger qb_p \in \mathbb{Z}_p - \{0\} \text{ and } N_{E_p}(b_p) \leq c_p N_{E_p}(q)^{d-1/2}.$$

For all but finitely many primes p , we can use Corollary 5.6 to choose b_p as above with $c_p = 1$; furthermore the set of exceptional p depends only on (R, \dagger) .

For all but finitely many p , we have $N_{E_p}(q) = 1$ (this time, the set of exceptions depends on q). If also $c_p = 1$, then the above bound says that $N_{E_p}(b_p) = 1$. For these p , Lemma 5.1 tells us that $b_p \in R_p^\times$.

Let

$$u_p = b_p^{-1}a \in E_p^\times.$$

Then

$$u_p u_p^\dagger = b_p^{-1} a a^\dagger b_p^{\dagger-1} = b_p^{-1} m q^{-1} b_p^{\dagger-1} = m (b_p^\dagger q b_p)^{-1} \in \mathbb{Q}_p^\times$$

so $u_p \in \mathbf{U}(\mathbb{Q}_p)$. Furthermore, for all but finitely many p , $a \in R_p^\times$ and $b_p \in R_p^\times$ so the u_p are components of an adelic element $\mathbf{u} \in \mathbf{U}(\mathbb{A}_f)$.

By [PR94] Theorem 5.1, the double coset space

$$\prod \mathbf{U}(\mathbb{Z}_p) \backslash \mathbf{U}(\mathbb{A}_f) / \mathbf{U}(\mathbb{Q})$$

is finite. Choose representatives $\mathbf{g}_1, \dots, \mathbf{g}_r$ for these double cosets. By multiplying them by suitable elements of \mathbb{Q}^\times , we clear denominators so that

$$\mathbf{g}_i \in \prod_p R \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

for each i .

We can decompose \mathbf{u} as

$$\mathbf{u} = \mathbf{y} \mathbf{g}_i x$$

for some $\mathbf{y} \in \prod_p \mathbf{U}(\mathbb{Z}_p)$, \mathbf{g}_i among our chosen double coset representatives and $x \in \mathbf{U}(\mathbb{Q})$.

Let $b = ax^{-1} \in E$. We claim that b satisfies the conditions of the proposition. At each prime p , we have that

$$b = ax^{-1} = b_p u_p x^{-1} = b_p y_p g_{i,p} \in R_p.$$

Hence $b \in \bigcap_p R_p = R$.

Next

$$b^\dagger q b = x^{\dagger-1} a^\dagger q a x^{-1} = m x^{\dagger-1} x^{-1}.$$

Now $x^{\dagger-1} x^{-1} \in \mathbb{Q}^\times$ because $x \in \mathbf{U}(\mathbb{Q})$, so we conclude that

$$b^\dagger q b \in \mathbb{Q}^\times.$$

In fact $b^\dagger q b \in \mathbb{Z} - \{0\}$ because b and q are both in R and $R \cap \mathbb{Q}^\times = \mathbb{Z} - \{0\}$.

Finally we have to bound

$$N_E(b) = \prod_p \left(N_{E_p}(b_p) N_{E_p}(y_p) N_{E_p}(g_{i,p}) \right).$$

For all p , $N_{E_p}(y_p) = 1$ because $y_p \in R_p^\times$.

For each i , $N_{E_p}(g_{i,p}) = 1$ for all but finitely many p , and so the following constant is well-defined:

$$c_0 = \max_{1 \leq i \leq r} \prod_p N_{E_p}(g_{i,p}).$$

Recall that we can choose \mathbf{g}_i depending only on (R, \dagger) so c_0 depends only on (R, \dagger, N_E) .

Using the bounds on $N_{E_p}(b_p)$ from Lemma 5.3 and Corollary 5.6, we get that

$$N_E(b) \leq c_0 \prod_p \left(c_p N_{E_p}(q)^{d/1-2} \right) = c_0 \left(\prod_p c_p \right) N_E(q)^{d-1/2}$$

and so Proposition 1.5 holds with $c = c_0 \prod_p c_p$. \square

Acknowledgements. I am grateful to Emmanuel Ullmo and Andrei Yafaev for useful conversations about the work in this paper. I would like to thank the MathOverflow user WKC who suggested the method of proof of Lemma 5.4. I also thank the referee for helpful comments.

During the writing of this paper, the author was supported by a doctoral grant from Université Paris Sud and by European Research Council grant 307364 “Some problems in Geometry of Shimura Varieties.”

REFERENCES

- [BO07] Y. Benoist and H. Oh, *Polar decomposition for p -adic symmetric spaces*, Int. Math. Res. Not. IMRN (2007), no. 24, Art. ID rnm121, 20.
- [HW93] A. G. Helminck and S. P. Wang, *On rationality properties of involutions of reductive groups*, Adv. Math. **99** (1993), no. 1, 26–96.
- [KMRT98] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998.
- [Kot92] R. E. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc. **5** (1992), no. 2, 373–444.
- [Lew82] D. W. Lewis, *Quaternionic skew-Hermitian forms over a number field*, J. Algebra **74** (1982), no. 1, 232–240.
- [Mil86] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.
- [Mum70] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Oxford University Press, London, 1970.
- [MW93] D. Masser and G. Wüstholz, *Isogeny estimates for abelian varieties, and finiteness theorems*, Ann. of Math. (2) **137** (1993), no. 3, 459–472.
- [O'M63] O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften, Bd. 117, Academic Press Inc., Publishers, New York, 1963.
- [Orr15] M. Orr, *Families of abelian varieties with many isogenous fibres*, J. Reine Angew. Math. **705** (2015), 211–231.
- [Pin05] R. Pink, *A combination of the conjectures of Mordell-Lang and André-Oort*, Geometric methods in algebra and number theory, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, pp. 251–282.
- [PR94] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994.
- [Sch85] W. Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften, vol. 270, Springer-Verlag, Berlin, 1985.
- [Shi63] G. Shimura, *Arithmetic of alternating forms and quaternion hermitian forms*, J. Math. Soc. Japan **15** (1963), 33–65.
- [Shi97] ———, *Euler products and Eisenstein series*, CBMS Regional Conference Series in Mathematics, vol. 93, Washington, DC, 1997.