TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 347, Number 7, July 1995

PRINCIPALLY POLARIZED ORDINARY ABELIAN VARIETIES OVER FINITE FIELDS

EVERETT W. HOWE

ABSTRACT. Deligne has shown that there is an equivalence from the category of ordinary abelian varieties over a finite field k to a category of $\mathbf{Z}$-modules with additional structure. We translate several geometric notions, including that of a polarization, into Deligne's category of $\mathbf{Z}$-modules. We use Deligne's equivalence to characterize the finite group schemes over k that occur as kernels of polarizations of ordinary abelian varieties in a given isogeny class over k. Our result shows that every isogeny class of simple odd-dimensional ordinary abelian varieties over a finite field contains a principally polarized variety. We use our result to completely characterize the Weil numbers of the isogeny classes of two-dimensional ordinary abelian varieties over a finite field that do not contain principally polarized varieties. We end by exhibiting the Weil numbers of several isogeny classes of absolutely simple four-dimensional ordinary abelian varieties over a finite field that do not contain principally polarized varieties.

1. INTRODUCTION

Every isogeny class of abelian varieties over an algebraically closed field contains a principally polarized variety, but very little is known about what happens over non-algebraically-closed fields. In this paper we consider isogeny classes of ordinary abelian varieties over finite fields, and we give an explicit criterion for deciding whether such an isogeny class contains a principally polarized variety.

Let k be a finite field with q elements and let $\mathscr{C}$ be an isogeny class of ordinary abelian varieties over k. For every variety A in $\mathscr{C}$ we let R_A be the subring of $\operatorname{End} A$ that is generated over $\mathbf{Z}$ by the qth-power Frobenius endomorphism F of A and the Verschiebung endomorphism $V = q/F$ of A. An isogeny $A \to B$ defines an isomorphism $R_A \to R_B$ that identifies the Frobenius endomorphisms of the two varieties, so the ring R_A is an invariant of the isogeny class $\mathscr{C}$; we denote this ring by $R_{\mathscr{C}}$, and we denote its subring $\mathbf{Z}[F+V]$ by $R_{\mathscr{C}}^+$. Deligne has defined an equivalence from the category of ordinary abelian varieties over k to a certain category of $\mathbf{Z}$-modules with additional structure. In §4 we will use this equivalence to associate to every polarization λ of a variety in $\mathscr{C}$ a finite $R_{\mathscr{C}}$-module whose module structure determines the finite group scheme $\ker\lambda$ (see the last part of §4, from Lemma 4.13 onward); in particular, the rank of $\ker\lambda$ is equal to the cardinality of the module

Received by the editors September 22, 1994.
1991 *Mathematics Subject Classification.* Primary 14G15; Secondary 11G10, 11G25.
The author was supported in part by a United States Department of Education National Need Fellowship.

associated to λ. In §5 we will associate functorially to $\mathscr{C}$ a finite two-torsion group $\mathscr{B}(\mathscr{C})$ and a homomorphism from the Grothendieck group $G(R_{\mathscr{C}}^+)$ of finite length $R_{\mathscr{C}}^+$-modules to $\mathscr{B}(\mathscr{C})$. We will define a particular element $I_{\mathscr{C}}$ of $\mathscr{B}(\mathscr{C})$, and at the end of §5 we will prove the following theorem.

(1.1) **Theorem.** *The Jordan-Hölder isomorphism classes of the $R_{\mathscr{C}}$-modules that come from polarizations of elements of $\mathscr{C}$ are exactly the Jordan-Hölder isomorphism classes that contain $R_{\mathscr{C}}$-modules of the form $M \otimes_{R_{\mathscr{C}}^+} R_{\mathscr{C}}$, where M is an $R_{\mathscr{C}}^+$-module whose image in $\mathscr{B}(\mathscr{C})$ is equal to $I_{\mathscr{C}}$. In particular, there is a principally polarized variety in $\mathscr{C}$ if and only if $I_{\mathscr{C}} = 0$.*

What makes this result useful is that it is possible to calculate the group $\mathscr{B}(\mathscr{C})$ and the element $I_{\mathscr{C}}$ in any specific case, and for isogeny classes of simple varieties we can even give a quite explicit general criterion for deciding whether $I_{\mathscr{C}}$ is zero (see Corollary 11.4). Loosely speaking, our criterion shows that it is very easy for $I_{\mathscr{C}}$ to be zero, and in §11 we will use our criterion to prove the following surprising result.

(1.2) **Theorem.** *Let $\mathscr{C}$ be an isogeny class of simple odd-dimensional ordinary abelian varieties over a finite field. Then there is a principally polarized variety in $\mathscr{C}$.*

In §12 we will consider isogeny classes of two-dimensional ordinary abelian varieties. Every such isogeny class $\mathscr{C}$ corresponds via the result of Honda and Tate (reviewed in §3 below) to a polynomial $h_{\mathscr{C}}$ of the form $X^4 + aX^3 - bX^2 + aqX + q^2$, where q is the cardinality of the finite field k. In §12 we will prove the following theorem, which should be compared with the results in [1, §5.4].

(1.3) **Theorem.** *Let q be a power of a prime p, let k be a field with q elements, let a and b be integers, and let*

$$h = X^4 + aX^3 - bX^2 + aqX + q^2.$$

Then $h = h_{\mathscr{C}}$ for an isogeny class $\mathscr{C}$ of two-dimensional ordinary abelian varieties over k that does not contain a principally polarized variety if and only if $q = a^2 + b$ and b is a positive integer, coprime to q, all of whose prime divisors are 1 modulo 3.

In §13 we will use Theorem 1.3 to prove that except for the isogeny classes, characterized in Theorem 1.3, that do not contain a principally polarized variety, *every* isogeny class of two-dimensional ordinary abelian varieties over a finite field k contains the Jacobian of a curve over k—this is Theorem 13.3, which extends a theorem of Rück ([16]).

It is natural to wonder whether there are theorems for arbitrary abelian varieties over a finite field analogous to the results proven in this paper for ordinary abelian varieties. In a forthcoming paper ([7]) we will show that a version of Theorem 1.1 does exist for arbitrary abelian varieties over a finite field; the problem is that there is not as yet a method for computing $I_{\mathscr{C}}$ in the general case. However, Theorem 1.2 does generalize to arbitrary abelian varieties over a finite field.

The plan of the present paper is as follows: In §2 we will review the definitions of Grothendieck groups and Chow groups. In §3 we will use the general result of Honda and Tate on isogeny classes of abelian varieties over finite fields ([6],

[19]) to show that isogeny classes of ordinary abelian varieties over finite fields correspond to polynomials of a certain type; we will call these polynomials *ordinary Weil polynomials.* In §4 we will recall Deligne's equivalence of categories and we will see how the concept of a polarization translates to his category of **Z**-modules with extra structure. We will use the results of §4 throughout the rest of the paper. In §5 we will define the obstruction group $\mathscr{B}(\mathscr{C})$ and the obstruction element $I_{\mathscr{C}}$ of Theorem 1.1, and we will show how the theorem follows from a number of propositions, which we will prove in §§6, 7, and 8. In §§9, 10, and 11 we will show how $\mathscr{B}(\mathscr{C})$ and $I_{\mathscr{C}}$ can be calculated from the Weil polynomial associated to $\mathscr{C}$. We will apply the techniques developed in these sections to the case of two-dimensional varieties in §12, where we will prove Theorem 1.3. Finally, in §13 we will use our results to construct the Weil polynomials of isogeny classes of absolutely simple four-dimensional ordinary abelian varieties that do not contain principally polarized varieties.

Conventions and notation. If A and B are varieties over a field k, then when we speak of a morphism from A to B we mean always a morphism *defined over* k. For instance, if A is an abelian variety over a field k, and if $\overline{k}$ is an algebraic closure of k, then what we call $\operatorname{End} A$ some authors would call $\operatorname{End}_k A$, and what we call $\operatorname{End}(A \times_k \overline{k})$ some authors would call $\operatorname{End} A$.

All rings are understood to be commutative with identity unless otherwise noted.

A *form* from an abelian group M to an abelian group N is a pairing $M \times M \to N$. Most of our nomenclature pertaining to pairings and forms will be standard; thus, for instance, if R is a ring with an involution $r \mapsto \overline{r}$ and if p is a form from an R-module M to an R-module N, then we will say that p is *R-sesquilinear* if we have $p(r\ell, m) = rp(\ell, m) = p(\ell, \overline{r}m)$ for all $r \in R$ and $\ell, m \in M$. However, we will use one term that may not be so common: If R is a ring with an involution and if p is a form from an R-module M to an abelian group N, then we say that p is *R-semi-balanced* if $p(r\ell, m) = p(\ell, \overline{r}m)$ for all $r \in R$ and $\ell, m \in M$. We will sometimes omit the R- from terms like *R-semi-balanced* and *R-sesquilinear* if the ring is clear from context.

Acknowledgments. This paper is based on a portion of the author's doctoral dissertation, written at the University of California, Berkeley; the author thanks his advisor, H.W. Lenstra, Jr., for his encouragement, advice, and support, without which this paper would not have been written. The author also thanks J. Milne for his helpful comments. Some of the work presented in this paper was done while the author was visiting the Université de Franche-Comté in Besançon, France; the author thanks E. Bayer, L. Fainsilber, and the many others in Besançon who made his visit there enjoyable and productive for their hospitality. The number-theoretic calculating program PARI/GP, by C. Batut, D. Bernardi, H. Cohen, and M. Olivier, was of great help in the construction of many of the examples in this paper.

2. Background: Grothendieck groups and Chow groups

Some of the ideas and results of this paper are best expressed in terms of Grothendieck groups and Chow groups. In this section we will review the definitions of these groups. We will only define Chow groups for a special class of rings, called *orders*, that we will define below.

Let R be a ring. We say that an R-module M is *finite* if it has finite length. Let $\mathscr{M}(R)$ denote the free abelian group on the isomorphism classes of finite R-modules. Let $G(R)$ be the quotient group of $\mathscr{M}(R)$ by the subgroup generated by the expressions $M - M' - M''$ for all exact sequences of R-modules $0 \to M' \to M \to M'' \to 0$. We call $G(R)$ the *Grothendieck group (of finite length modules)* of R. It is not hard to see that $G(R)$ is a free abelian group on the simple R-modules. For every finite R-module M, we let $[M]_R$ denote the image of M in $G(R)$. Two R-modules M and N are *Jordan-Hölder isomorphic* if $[M]_R = [N]_R$. An element P of $G(R)$ is *effective* if there is an R-module M such that $P = [M]_R$. If we write $P = \sum n_i[S_i]_R$ as a sum of multiples of distinct simple R-modules S_i, then P is effective if and only if each n_i is non-negative. If P and Q are two elements of $G(R)$, we write $P \geq Q$ if $P - Q$ is effective. The *length* of P, denoted length(P), is the integer $\sum n_i$. Clearly, length is a homomorphism from $G(R)$ to $\mathbf{Z}$, and for every finite R-module M the length of $[M]_R$ is the usual length of M as an R-module.

An *order* is a ring R that has no nilpotent elements and that is free and finitely generated as a $\mathbf{Z}$-module. Let R be an order, and let K be the total quotient ring $Q(R)$ of R, that is, the localization of R at the multiplicative set of non-zero-divisors. The ring K is a finite product of number fields, and R can be viewed as a subset of K. In fact, R is a subring of finite index in $\mathscr{O}_K$, the integral closure of $\mathbf{Z}$ in K. Conversely, if K is a finite product of number fields and R is a subring of finite index in $\mathscr{O}_K$, then R is an order. In this situation we say that R is an *order of* K, or an *order in* K. Notice that K is equal to the tensor product $R \otimes \mathbf{Q}$.

Suppose R and S are orders and $\psi: R \to S$ is a ring homomorphism. Then S is finitely generated as an R-module, so every finite S-module can also be viewed as a finite R-module. This gives us a homomorphism from $\mathscr{M}(S)$ to $\mathscr{M}(R)$, and since an exact sequence of S-modules is also an exact sequence of R-modules, we get a homomorphism $G(\psi)$, the *norm*, from $G(S)$ to $G(R)$. One can easily verify that G is a contravariant functor from the category of orders to the category of abelian groups. On the other hand, if M is a finite R-module then $M \otimes_R S$ is a finite S-module, so the tensor product gives us a homomorphism from $\mathscr{M}(R)$ to $\mathscr{M}(S)$. If S is flat over R, then the tensor product takes short exact sequences of R-modules to short exact sequences of S-modules, so the tensor product induces a homomorphism ψ_* from $G(R)$ to $G(S)$. If it is clear from context which map ψ from R to S we are referring to, we will sometimes write $N_{S/R}$ for $G(\psi)$. If in addition S is flat over R, we will sometimes write $t_{S/R}$ for ψ_*.

Suppose R is an order and let K be the ring $Q(R)$. We define a homomorphism $\mathrm{Pr}_R: K^* \to G(R)$ from the group of units of K to $G(R)$ as follows: Given an $x \in K^*$, we write $x = a/b$ for some non-zero-divisors a and b in R and we define $\mathrm{Pr}_R(x)$ to be $[R/aR]_R - [R/bR]_R$. It is easy to check that Pr_R is well-defined. The elements of $G(R)$ in the image of Pr_R are called *principal* elements. The *Chow group* of R, denoted $\mathrm{Ch}(R)$, is the group $G(R)/\mathrm{Pr}_R(K^*)$, the cokernel of Pr_R.

Let R and S be orders and let ψ be a ring homomorphism from R to S, so that S can be viewed as an R-module. Let $K = Q(R)$ and let $L = Q(S)$.

Then L is a locally free K-module of finite rank, and since $K = \prod_{i\in I} K_i$ is a product of fields we can write $L = \prod_{i\in I} L_i$ as a product of K_i-algebras. This gives us a norm map $N_{L/K}$ from L to K defined by sending an element x of L to the element of K which on each factor K_i is the determinant of the endomorphism of L_i obtained by restriction from the multiplication-by-x endomorphism of L. The norm of a unit of L is a unit of K, and we have the following well-known lemma.

(2.1) **Lemma.** *In the above notation,* $N_{S/R}(\mathrm{Pr}_S(x)) = \mathrm{Pr}_R(N_{L/K}(x))$ *for every unit* x *of* L.

Proof. First of all, we need only prove the statement of the lemma for $x \in L^*$ such that $x \in S$ and $N_{L/K}(x) \in R$, since these x generate L^*. For such x, the statement of the lemma is that $[S/xS]_R = [R/N_{L/K}(x)R]_R$. Let $A = \mathscr{O}_K$, let $B = \mathscr{O}_L$, and consider the following diagram of R-modules:

$$\begin{array}{ccc} xB & \subset & B \\ \cup & & \cup \\ xS & \subset & S. \end{array}$$

Since the finite R-modules xB/xS and B/S are isomorphic, we see that $[B/xB]_R = [S/xS]_R$. Similarly, we see that $[A/N_{L/K}(x)A]_R = [R/N_{L/K}(x)R]_R$, so we will be done if we can show that $[B/xB]_A = [A/N_{L/K}(x)A]_A$. To prove this equality it will be enough to prove the corresponding equality for every localization of A, so pick a prime $\mathfrak{p}$ of A and replace A and B with their localizations at $\mathfrak{p}$. Now A is a regular local ring and hence a principal ideal domain, and B is a finitely generated free A-module. Our equality now follows from [18, §I.5, Lemma 3, p. 17]. □

Lemma 2.1 shows that the norm from $G(S)$ to $G(R)$ induces a homomorphism from $\mathrm{Ch}(S)$ to $\mathrm{Ch}(R)$ which we will again call the norm and denote by $\mathrm{Ch}(\psi)$. Thus Ch is a contravariant functor from the category of orders to the category of abelian groups.

Suppose R is an order and let $K = Q(R)$. Let K_0 be the subgroup of K^* consisting of elements $x \in K^*$ such that $\varphi(x) > 0$ for all ring homomorphisms $\varphi: K \to \mathbf{R}$ from K to the real numbers. The *narrow Chow group* of R, denoted $\mathrm{Ch}^+(R)$, is the group $G(R)/\mathrm{Pr}(K_0)$, the cokernel of $\mathrm{Pr}|_{K_0}$. Lemma 2.1 shows that Ch^+ gives a contravariant functor from the category of orders to the category of abelian groups.

An order R is *totally real* if every ring homomorphism from R to the complex numbers maps R into the real numbers. An order R is *totally imaginary* if there is no ring homomorphism from R to the real numbers. Notice that if R is a totally imaginary order then $K_0 = K^*$, so that $\mathrm{Ch}^+(R) = \mathrm{Ch}(R)$. A *CM-field* is a totally imaginary quadratic extension of a totally real number field. An order R is a *CM-order* if $Q(R)$ is a product of CM-fields. If K is a product of CM-fields, let K^+ denote the product of the maximal real subfields of the factors of K; we view K^+ as a subset of K. Given a CM-order R, let R^+ denote the intersection of R with $Q(R)^+$; the order R^+ is totally real.

We end this section with a simple example.

(2.2) **Example.** Suppose K is a totally real subfield of a totally imaginary field L. Then $\mathrm{Ch}(\mathscr{O}_L) = \mathrm{Cl}(L)$, the ideal class group of L, and $\mathrm{Ch}^+(\mathscr{O}_K) =$

$\mathrm{Cl}^+(K)$, the narrow class group of K. The norm from $\mathrm{Ch}(\mathscr{O}_L)$ to $\mathrm{Ch}^+(\mathscr{O}_K)$ is the usual norm of ideal class groups.

3. Isogeny classes of ordinary abelian varieties over finite fields

Suppose k is a finite field with q elements. If A is an abelian variety over k, we denote by h_A the characteristic polynomial in $\mathbf{Z}[X]$ of the Frobenius endomorphism of A. The degree of the polynomial h_A is twice the dimension of A, and Weil's theorem for curves says that every complex root of h_A is a *Weil q-number*, that is, an algebraic integer π such that $|\varphi(\pi)| = q^{1/2}$ for every embedding φ of $\mathbf{Q}(\pi)$ into $\mathbf{C}$. The theorem of Honda and Tate (see [6], [19]) says that the map that sends a simple abelian variety A over k to the set of complex roots of h_A induces a bijection between the set of isogeny classes of simple abelian varieties over k and the set of Galois conjugacy classes of Weil q-numbers. In this section we will state a slight variant of the Honda-Tate theorem that works only for ordinary abelian varieties. We begin with two definitions.

(3.1) **Definition** (see [3, §2]). Let q be a power of a prime number p, let k be a field with q elements, and let $\overline{k}$ be an algebraic closure of k. A g-dimensional abelian variety A over k is *ordinary* if the following equivalent conditions are satisfied:

(a) A has exactly p^g points over $\overline{k}$ of order dividing p.
(b) The connected component of the kernel of the multiplication-by-p map on A is of multiplicative type.
(c) At least half of the roots of h_A in $\overline{\mathbf{Q}}_p$, counting multiplicities, are p-adic units.
(d) The middle coefficient of h_A is not divisible by p.

(The *middle coefficient* of a polynomial in X of degree $2g$ is the coefficient of X^g.)

(3.2) **Definition.** Let q be a power of a prime number p. An *ordinary Weil q-polynomial* is a monic $h \in \mathbf{Z}[X]$ of even degree such that

(a) all of the roots of h in $\mathbf{C}$ have magnitude $q^{1/2}$, and
(b) the middle coefficient of h is not divisible by p.

From these definitions we see that if A is an ordinary abelian variety over $\mathbf{F}_q$, then h_A is an ordinary Weil q-polynomial. In fact, all ordinary Weil q-polynomials arise in this way.

(3.3) **Theorem** (Honda-Tate for ordinary varieties). *Let q be a power of a prime number p and let k be a field with q elements. The map that sends an ordinary abelian variety A over k to the polynomial h_A induces a bijection between the set of isogeny classes of ordinary abelian varieties over k and the set of ordinary Weil q-polynomials. Under this bijection, isogeny classes of simple ordinary abelian varieties correspond to irreducible ordinary Weil q-polynomials.*

Proof. This theorem follows easily from the standard Honda-Tate theorem ([19, Théorème 1, p. 96]) and from the fact that for a simple ordinary abelian variety A the polynomial h_A is irreducible. □

Finally, it is useful to note that ordinary Weil q-polynomials have a special form.

(3.4) **Proposition.** *Suppose that*

$$h = X^{2g} + a_{2g-1}X^{2g-1} + \cdots + a_1X + a_0$$

is an ordinary Weil q-polynomial. Then $X^{2g}h(q/X) = q^g h(X)$; *we have* $a_0 = q^g$, *and for* $i = 1, \ldots, g$ *we have* $a_i = q^{g-i}a_{2g-i}$.

Proof. If h had a real root then it would have a $\mathbf{Q}$-irreducible factor of the form $X \pm q^{1/2}$ or $X^2 - q$, depending on whether or not $q^{1/2}$ is an integer, and no ordinary Weil q-polynomial can have such a factor. Thus h factors over $\mathbf{R}$ as a product of polynomials of the form $X^2 - tX + q$, so we have $a_0 = q^g$. Since the complex roots of h all have magnitude $q^{1/2}$, it follows that $X^{2g}h(q/X) = a_0h(X) = q^g h(X)$. The statement about the symmetry of the coefficients of h follows immediately from this equality. □

4. Ordinary abelian varieties over finite fields

In the previous section we presented a slight variant of the theorem of Honda and Tate that provides a simple description of isogeny classes of ordinary abelian varieties over a finite field. The result of Deligne presented in [3] can be viewed as an extension of this variant of the Honda-Tate theorem: For every ordinary abelian variety in an isogeny class corresponding via Theorem 3.3 to an ordinary Weil polynomial h, Deligne provides a finitely generated free $\mathbf{Z}$-module and an endomorphism of the module having characteristic polynomial h. In fact, Deligne shows that the category of ordinary abelian varieties over $\mathbf{F}_q$ is equivalent to a category $\mathscr{L}_q$ whose objects are finitely generated free $\mathbf{Z}$-modules provided with an endomorphism having certain properties. In this section, we will review the results of [3] and see how the concept of a polarization can be expressed in the category $\mathscr{L}_q$. We begin by defining the category $\mathscr{L}_q$.

(4.1) **Definition.** If q is a power of a prime p, let $\mathscr{L}_q$ be the category of pairs (T, F) where T is a finitely generated free $\mathbf{Z}$-module and F is an endomorphism of T satisfying the following conditions:

(a) The endomorphism $F \otimes \mathbf{Q}$ of $T \otimes \mathbf{Q}$ is semi-simple, and its eigenvalues in $\mathbf{C}$ have magnitude $q^{1/2}$.
(b) At least half of the roots of the characteristic polynomial of F in $\overline{\mathbf{Q}}_p$, counting multiplicities, are p-adic units.
(c) There is an endomorphism V of T such that $FV = q$.

A morphism from (T, F) to (T', F') is a homomorphism $\psi: T \to T'$ of $\mathbf{Z}$-modules such that $\psi \circ F = F' \circ \psi$.

We refer to the objects of $\mathscr{L}_q$ as *Deligne q-modules*, or as *Deligne modules*, if q is clear from context. If B is a Deligne module, then B consists of a $\mathbf{Z}$-module and an endomorphism; we let T_B denote the module, and F_B the endomorphism. We will write V_B for the endomorphism q/F_B. It follows from the definition that T_B has even rank as a $\mathbf{Z}$-module and that *exactly* half of the roots of the characteristic polynomial of F in $\overline{\mathbf{Q}}_p$, counting multiplicities, are

p-adic units—see [3, Théorème (part d), pp. 240–241]. The *dimension* of B is half of the $\mathbf{Z}$-rank of T_B.

Deligne's theorem says that the category of ordinary abelian varieties over $\mathbf{F}_q$ is equivalent to the category $\mathscr{L}_q$. To describe the functor providing the equivalence, we need to set some notation. Let q be a power of a prime p, let k be a field with q elements, let $\overline{k}$ be an algebraic closure of k, let $W = W(\overline{k})$ be the ring of Witt vectors over $\overline{k}$, let $\varepsilon: W \hookrightarrow \mathbf{C}$ be an embedding of W into the complex numbers, let v be the p-adic valuation on $\overline{\mathbf{Q}} \subset \mathbf{C}$ obtained from ε, and let $\mathbf{Z}(1)$ be the subgroup $2\pi i\mathbf{Z}$ of $\mathbf{C}$. If G is an abelian group, then for every positive integer m we denote by $G[m]$ the m-torsion of G, and for every prime ℓ we denote by $T_\ell(G)$ the ℓ-adic Tate module of G; that is, $T_\ell(G) = \operatorname{proj\,lim} G[\ell^n]$. The exponential map induces an isomorphism between $\mathbf{Z}(1) \otimes \mathbf{Z}_\ell$ and $T_\ell(\mathbf{C}^*)$.

Deligne's functor is defined as follows: Let A be an ordinary abelian variety over k and let Frob_A be the Frobenius morphism on A. Let $A^\#$ be the canonical Serre-Tate lifting of A to W and let $F^\#$ be the lifting of Frob_A to $A^\#$ (for information on the Serre-Tate lifting, see [8, §2, pp. 148–158], [10, §V.3, pp. 171–174], or [13].) Let $T(A)$ denote the integer homology of the complex abelian variety $A_{\mathbf{C}}$ obtained from $A^\#$ by extension of scalars from W to $\mathbf{C}$ via ε; that is, let $T(A) = H_1(A^\# \otimes_\varepsilon \mathbf{C})$. Finally, let $F(A)$ denote the endomorphism of $T(A)$ induced by $F^\#$. The characteristic polynomial of $F(A)$ is equal to h_A.

(4.2) **Theorem** (Deligne). *The functor $A \mapsto (T(A), F(A))$ is an equivalence of categories between the category of ordinary abelian varieties over k and the category $\mathscr{L}_q$.*

Proof. See [3, Théorème, pp. 240–241]. □

If $B = (T, F)$ is an element of $\mathscr{L}_q$ and if A is the corresponding abelian variety over k, then $T = H_1(A_{\mathbf{C}})$, so that $T \otimes \mathbf{R}$ is identified with the Lie algebra of $A_{\mathbf{C}}$ and is thus given a complex structure. Following Serre, Deligne gives a proposition describing in another way this complex structure.

(4.3) **Proposition.** *The complex structure defined on $T \otimes \mathbf{R}$ as above is characterized by the following two properties:*

(a) *The endomorphism F is $\mathbf{C}$-linear.*
(b) *The eigenvalues of F have positive valuation under the p-adic valuation v defined above.*

Proof. See [3, Proposition, p. 242]. □

Suppose B is a Deligne module. We say that B is *simple* if $F_B \otimes \mathbf{Q}$ is a simple endomorphism of $T_B \otimes \mathbf{Q}$. If C is also a Deligne module and $\psi: B \to C$ is a morphism, we say that ψ is an *isogeny* if $\psi \otimes \mathbf{Q}$ is an isomorphism between $T_B \otimes \mathbf{Q}$ and $T_C \otimes \mathbf{Q}$. It is easy to see that under Deligne's functor simple ordinary abelian varieties correspond to simple Deligne modules and isogenies correspond to isogenies.

There are three other concepts from the category of ordinary abelian varieties that we would like to translate into the category $\mathscr{L}_q$. These are the concepts of the dual of a variety, of polarizations of a variety, and of kernels of isogenies between varieties.

(4.4) **Definition.** If $B = (T, F)$ is an element of $\mathscr{L}_q$, we define the *dual* of B to be $\hat{B} = (\hat{T}, \hat{F})$, where $\hat{T}$ is the $\mathbf{Z}$-module $\mathrm{Hom}_{\mathbf{Z}}(T, \mathbf{Z})$ and where $\hat{F}$ is the endomorphism of $\hat{T}$ such that for all $\psi \in \hat{T}$ and $t \in T$ we have $(\hat{F}\psi)(t) = \psi(Vt)$.

(4.5) **Proposition.** *Let A/k be an ordinary abelian variety with dual variety $\hat{A}/k$. Then $(T(\hat{A}), F(\hat{A}))$ is the dual of $(T(A), F(A))$.*

Proof. From the description of the dual of a complex abelian variety ([12, §9, p. 86], [15, §4, pp. 93–94]) we see that there is a perfect pairing $e: T(A) \times T(\hat{A}) \to \mathbf{Z}(1)$, and from [3] we know that for every prime $\ell \neq p$, when we tensor e with $\mathbf{Z}_\ell$, identify $\mathbf{Z}(1) \otimes \mathbf{Z}_\ell$ with $T_\ell(\mathbf{C}^*)$, and reduce from the Witt vectors to $\bar{k}$, we obtain the Weil pairing $e_\ell: T_\ell(A) \times T_\ell(\hat{A}) \to T_\ell(\bar{k}^*)$. The Weil pairing is Galois invariant, so that if σ is the Frobenius automorphism of $\bar{k}/k$ we have $e_\ell(\sigma x, \sigma y) = e_\ell(x, y)^q$. Since for $\bar{k}$-valued points x of A we have $\sigma x = \mathrm{Frob}(x)$, we see that the pairing e must satisfy $e(F(A)s, F(\hat{A})t) = q \cdot e(s, t)$ for all $s \in T(A)$ and $t \in T(\hat{A})$. From this we see that $e(s, F(\hat{A})t) = e(V(A)s, t)$. Thus the pairing e provides an isomorphism between $(T(\hat{A}), F(\hat{A}))$ and the dual of $(T(A), F(A))$. □

Our next task is to translate the notion of a polarization into the language of the category $\mathscr{L}_q$. Recall that a polarization of an abelian variety A is an isogeny from A to $\hat{A}$ that in a certain sense comes from an ample invertible sheaf (see [11, §13]). Over the complex numbers, this condition on the isogeny boils down to the condition that a certain bilinear form be a non-degenerate alternating Riemann form. It is the latter criterion that allows us to determine the correct definition of a polarization of an element of $\mathscr{L}_q$. We begin by setting some notation that we will use throughout the rest of the paper.

(4.6) *Notation.* Suppose $B = (T, F)$ is an element of $\mathscr{L}_q$. Let $R = R_B$ be the subring $\mathbf{Z}[F, V]$ of $\mathrm{End}\, B$ and let $K = K_B$ be the $\mathbf{Q}$-algebra $R \otimes \mathbf{Q}$. It follows from the examples on page 97 of [19], or from [20, Proposition 7.1, p. 553], that K is a product of CM-fields, and clearly R is an order in K. The involution $^-$ of K that is complex conjugation on each of the factors of K interchanges F and V. Recall that our choice of an embedding $\varepsilon: W(\bar{k}) \hookrightarrow \mathbf{C}$ gave us a p-adic valuation v on $\bar{\mathbf{Q}} \subset \mathbf{C}$; this valuation provides K with some additional structure. Namely, we let

$$\Phi = \Phi_B = \{\varphi: K \to \mathbf{C} \mid v(\varphi(F)) > 0\};$$

Φ is a *CM-type* of K—that is, Φ is a set of half of all the ring homomorphisms from K to $\mathbf{C}$, no two of which are complex conjugates. Notice that Φ depends on our choice of ε.

(4.7) **Definition.** Let K be a product of CM-fields and let Φ be a CM-type of K. An element x of K is *totally imaginary* if $\bar{x} = -x$. A totally imaginary x of K is *Φ-positive* (respectively, *Φ-non-negative, Φ-negative, Φ-non-positive*) if $\varphi(x)/i$ is positive (respectively, non-negative, negative, non-positive) for all $\varphi \in \Phi$.

Suppose λ is an isogeny from $B = (T, F)$ to $\hat{B}$. Notice that λ gives us a non-degenerate R-semi-balanced form b from T to $\mathbf{Z}$, defined by $b(s, t) =$

$\lambda(t)(s)$. Conversely, every non-degenerate R-semi-balanced form b from T to $\mathbf{Z}$ gives us an isogeny from B to $\widehat{B}$. Also, from [9, Theorem I.7.4.1, p. 44] we see that for every such b there is a unique non-degenerate K-sesquilinear form S from $T_{\mathbf{Q}} = T \otimes \mathbf{Q}$ to K such that $b \otimes \mathbf{Q} = \mathrm{Tr}_{K/\mathbf{Q}} \circ S$, and clearly different forms b give rise to different forms S. We will call b the *semi-balanced form associated to* λ, and S the *sesquilinear form associated to* λ. Similarly, we will refer to the isogeny λ obtained from a semi-balanced b or from a sesquilinear S (with $\mathrm{Tr}_{K/\mathbf{Q}}(S(T, T)) \subset \mathbf{Z}$) as the *isogeny associated to* b or S.

(4.8) **Definition.** Let $B = (T, F)$ be an element of $\mathscr{L}_q$. A *polarization* of B is an isogeny λ from B to its dual such that the non-degenerate sesquilinear form S associated to λ satisfies the following two conditions:

(a) S is skew-Hermitian, and

(b) $S(t, t)$ is Φ_B-non-positive for all $t \in T$.

(4.9) **Proposition.** *Let A be an ordinary abelian variety over $\mathbf{F}_q$ corresponding to an element $B = (T, F)$ of $\mathscr{L}_q$. Let μ be an isogeny from A to $\widehat{A}$, and let λ be the corresponding isogeny from B to $\widehat{B}$. Then μ is a polarization of A if and only if λ is a polarization of B.*

Proof. First of all, we know from [3] that μ is a polarization of A if and only if $\mu_{\mathbf{C}}$ is a polarization of the complex abelian variety $A_{\mathbf{C}}$. Now, $A_{\mathbf{C}}$ is analytically isomorphic to the complex torus $T_{\mathbf{R}}/T$, and from the explicit description of the dual variety of $A_{\mathbf{C}}$ ([12, §9, p. 86], [15, §4, pp. 93–94]) we see that an isogeny from $A_{\mathbf{C}}$ to its dual corresponds to a non-degenerate $\mathbf{C}$-semi-balanced form $E: T_{\mathbf{R}} \times T_{\mathbf{R}} \to \mathbf{R}$ such that $E(T, T) \subset \mathbf{Z}$. There is a bijection between the set of such E and the set of non-degenerate sesquilinear forms $H: T_{\mathbf{R}} \times T_{\mathbf{R}} \to \mathbf{C}$ with $H(T \times T) \subset \mathbf{R} + i\mathbf{Z}$, given by sending a form E to the form H defined by $H(x, y) = E(ix, y) + iE(x, y)$. We know from [15, §3] that the isogeny $\mu_{\mathbf{C}}$ from $A_{\mathbf{C}}$ to $\widehat{A}_{\mathbf{C}}$ is a polarization if and only if its associated form H is a *Riemann form*, which means by definition that in addition to having the property that $H(T \times T) \subset \mathbf{R} + i\mathbf{Z}$, the form H must also be a positive definite Hermitian form. Equivalently, E must be an *alternating Riemann form*, which means by definition that in addition to satisfying the requirement that $E(T \times T) \subset \mathbf{Z}$, the form E must be alternating and have the property that the form $(x, y) \mapsto E(ix, y)$ be symmetric and positive definite.

The fact that ties all of the above information to our definition of a polarization of a Deligne module is that the non-degenerate $\mathbf{C}$-semi-balanced form E associated to μ is the non-degenerate R-semi-balanced form b associated to λ, tensored with $\mathbf{R}$; this follows from the definition of λ in terms of μ, found in [3]. Let S be the sesquilinear form associated to λ. Using the facts that $E = b \otimes \mathbf{R}$ and that $b \otimes \mathbf{Q} = \mathrm{Tr}_{K/\mathbf{Q}} \circ S$, we can write E as the composition

$$T_{\mathbf{R}} \times T_{\mathbf{R}} \xrightarrow{S \otimes \mathbf{R}} K \otimes \mathbf{R} \xrightarrow{\Phi} \mathbf{C}^d \xrightarrow{\mathrm{Tr}} \mathbf{R}, \tag{1}$$

where d is the cardinality of Φ_B, where $\Phi: K \otimes \mathbf{R} \cong \mathbf{C}^d$ is the map that sends $x \otimes 1$ to the d-tuple $(\varphi(x))_{\varphi \in \Phi_B}$, and where Tr is the trace map from $\mathbf{C}^d$ to $\mathbf{R}$ that sends a d-tuple of complex numbers to twice the sum of the real parts of its elements. Let $C: T_{\mathbf{R}} \times T_{\mathbf{R}} \to \mathbf{C}^d$ be the composition of $S \otimes \mathbf{R}$ and Φ. By Proposition 4.3, the map C is a $\mathbf{C}$-sesquilinear form from the $\mathbf{C}$-vector space $T_{\mathbf{R}}$ to $\mathbf{C}^d$.

Suppose that μ is a polarization, so that E is an alternating Riemann form. We would like to show that S satisfies the conditions of Definition 4.8. First, since $E(t, t) = 0$ for all $t \in T_{\mathbf{Q}}$ and since $E = b \otimes \mathbf{R}$, we have $b(t, t) = 0$ for all $t \in T_{\mathbf{Q}}$. Then for all s and t in $T_{\mathbf{Q}}$ we have

$$\begin{aligned}\mathrm{Tr}_{K/\mathbf{Q}}(S(s, t) + \overline{S(t, s)}) &= \mathrm{Tr}_{K/\mathbf{Q}}(S(s, t) + S(t, s)) \\ &= b(s + t, s + t) - b(s, s) - b(t, t) = 0,\end{aligned}$$

so that the sesquilinear form $(s, t) \mapsto S(s, t) + \overline{S(t, s)}$ on $T_{\mathbf{Q}}$ is not surjective on any factor of the product of fields K, and is therefore identically zero. This shows that S is skew-Hermitian.

Let φ be an element of Φ_B. The weak approximation theorem from number theory asserts that we can find a sequence $\{\alpha_j\}$ of elements of K^+ such that if ψ is an element of Φ_B, then $\lim_{j\to\infty} \psi(\alpha_j)$ is 0 if $\psi \neq \varphi$ and is 1 if $\psi = \varphi$. Then for every $t \in T_{\mathbf{Q}}$ we have

$$\begin{aligned}2\,\mathrm{Re}(i\varphi(S(t, t))) &= \mathrm{Tr}\, i \lim_{j\to\infty} \Phi(\alpha_j^2 S(t, t)) = \lim_{j\to\infty} \mathrm{Tr}\, i\Phi(S(\alpha_j t, \alpha_j t)) \\ &= \lim_{j\to\infty} \mathrm{Tr}\, iC(\alpha_j t, \alpha_j t) = \lim_{j\to\infty} \mathrm{Tr}\, C(i\alpha_j t, \alpha_j t) \\ &= \lim_{j\to\infty} E(i\alpha_j t, \alpha_j t) \geq 0\end{aligned}$$

so that $\varphi(S(t, t))$ is negative imaginary or zero. This is true for all $\varphi \in \Phi_B$, so that $S(t, t)$ is Φ-non-positive. Thus S satisfies the second condition of Definition 4.8, so that if μ is a polarization of A, then λ is a polarization of B.

On the other hand, suppose λ is a polarization of B, so that S is a skew-Hermitian form such that $S(t, t)$ is Φ-non-positive for all $t \in T$. Let E and H be the forms on $T_{\mathbf{R}}$ obtained from μ as above; we would like to show that H is a Riemann form. An easy calculation using the sequence (1) shows that for all t in $T_{\mathbf{Q}}$ we have $E(t, t) = 0$, and that the pairing from $T_{\mathbf{Q}}$ to $\mathbf{R}$ given by $(s, t) \mapsto E(is, t)$ is a positive semi-definite symmetric form. By continuity, we see that for all $t \in T_{\mathbf{R}}$ we have $E(t, t) = 0$, and that the pairing from $T_{\mathbf{R}}$ to $\mathbf{R}$ given by $(s, t) \mapsto E(is, t)$ is also symmetric and positive semi-definite. Thus H is a positive semi-definite Hermitian form, and we will be done if we can show that H is actually definite.

By [17, Theorem 7.6.3, p. 259] we can find a basis $\{x_1, \ldots, x_g\}$ for the $\mathbf{C}$-vector space $T_{\mathbf{R}}$ whose elements are pairwise orthogonal with respect to H. Since μ is an isogeny, H is non-degenerate, so for each $i = 1, \ldots, g$ we must have $H(x_i, x_i) > 0$. From this fact it follows easily that H is positive definite, so H is a non-degenerate Riemann form and μ is a polarization. □

(4.10) *Remark.* Suppose $\lambda: B \to \widehat{B}$ is an isogeny with associated semi-balanced form b and suppose ι is a Φ_B-positive element of R_B. Using ideas from the proof of Proposition 4.9, one can show that λ is a polarization if and only if b is alternating and the form $(x, y) \mapsto b(\iota x, y)$ on R_B is symmetric and positive definite. Thus one could take these latter conditions to be the definition of a polarization of a Deligne module. The advantage of this alternate definition is that it is reminiscent of the definition of an alternating Riemann form on a lattice in a complex vector space. The disadvantage is that it is not immediately clear that the definition is independent of the element ι.

We will see that the ring R_A is an important invariant of a Deligne module A. In fact, R_A is an isogeny invariant, because if A and B are Deligne modules, an isogeny from A to B gives us an isomorphism from R_A to R_B that takes F_A to F_B and V_A to V_B. Thus the following definition makes sense.

(4.11) **Definition.** Let $\mathscr{C}$ be an isogeny class of Deligne modules, and let A be an element of $\mathscr{C}$. Define $R_{\mathscr{C}}$ to be the ring R_A, and define elements $F_{\mathscr{C}}$ and $V_{\mathscr{C}}$ of $R_{\mathscr{C}}$ by taking them to be F_A and V_A. Define $K_{\mathscr{C}}$ to be the product of fields $R_{\mathscr{C}} \otimes \mathbf{Q}$.

Later in this section we will require the following simple lemma about the rings $R_{\mathscr{C}}$. Further information about these rings can be found in §9.

(4.12) **Lemma.** *Let $\mathscr{C}$ be an isogeny class of Deligne q-modules. The elements $F_{\mathscr{C}}$ and $V_{\mathscr{C}}$ of $R_{\mathscr{C}}$ generate the unit ideal of $R_{\mathscr{C}}$.*

Proof. Let $R = R_{\mathscr{C}}$, let $F = F_{\mathscr{C}}$, let $V = V_{\mathscr{C}}$, let g be the dimension of the Deligne modules in $\mathscr{C}$, and let h be the ordinary Weil q-polynomial corresponding via Theorems 3.3 and 4.2 to $\mathscr{C}$. Then h is the characteristic polynomial of F, so $h(F) = 0$. We may interpret this equality as an identity in $K = R \otimes \mathbf{Q}$, and by dividing the equality by F^g and using the relations among the coefficients of h given in Proposition 3.4, we see that the middle coefficient a_g of h can be written as a $\mathbf{Z}$-linear combination of powers of F and $V = q/F$. Thus, a_g is an element of the ideal of R generated by F and V, and since this ideal also contains $q = FV$, it contains 1 as well, because a_g is coprime to q. In other words, F and V generate the unit ideal of R. □

Our final task in this section is to show how the group-scheme structure of the kernel of an isogeny of ordinary abelian varieties over a finite field can be determined from properties of the corresponding isogeny of Deligne modules.

For the rest of the section, let q be a power of a prime p, let k be a finite field with q elements, let $\overline{k}$ be an algebraic closure of k, let $\mu: C \to D$ be an isogeny of ordinary abelian varieties over k, and let $\lambda: A \to B$ be the isogeny of Deligne modules corresponding to μ. Let $T = T_A$ and let $U = T_B$. Let $\mathscr{C}$ be the isogeny class of Deligne modules containing A and B, let $R = R_{\mathscr{C}}$, let $K = K_{\mathscr{C}}$, let $F = F_{\mathscr{C}}$, and let $V = V_{\mathscr{C}}$. From the isogeny λ we obtain an isomorphism $\lambda_{\mathbf{Q}} = \lambda \otimes \mathbf{Q}$ of the K-modules $T_{\mathbf{Q}} = T \otimes \mathbf{Q}$ and $U_{\mathbf{Q}} = U \otimes \mathbf{Q}$, and we also get an R-module homomorphism $\lambda_{\mathbf{Q}/\mathbf{Z}}$ from $T_{\mathbf{Q}/\mathbf{Z}} = T \otimes (\mathbf{Q}/\mathbf{Z})$ to $U_{\mathbf{Q}/\mathbf{Z}} = U \otimes (\mathbf{Q}/\mathbf{Z})$. The kernel of $\lambda_{\mathbf{Q}/\mathbf{Z}}$ is equal to $\lambda_{\mathbf{Q}}^{-1}(U)/T$, and is an R-module of finite cardinality.

(4.13) **Lemma.** *With notation as above, let M_{rr} be the sub-R-module of* $\ker \lambda_{\mathbf{Q}/\mathbf{Z}}$ *consisting of elements of order coprime to q, let $M_{r\ell}$ be the V-power torsion of* $\ker \lambda_{\mathbf{Q}/\mathbf{Z}}$, *and let $M_{\ell r}$ be the F-power torsion of* $\ker \lambda_{\mathbf{Q}/\mathbf{Z}}$. *Then the endomorphisms F and V of M_{rr} are invertible, the endomorphism F of $M_{r\ell}$ is invertible, and the endomorphism V of $M_{\ell r}$ is invertible. Also,*

$$\ker \lambda_{\mathbf{Q}/\mathbf{Z}} = M_{rr} \oplus M_{r\ell} \oplus M_{\ell r}.$$

Proof. The lemma follows immediately from Lemma 4.12 and the fact that $FV = q$. □

Let σ be the qth-power-raising automorphism of $\overline{k}/k$, so that the Galois group $\mathrm{Gal}(\overline{k}/k)$ is freely generated as a profinite group by σ. Suppose M

is a finite abelian group and α is an automorphism of M. We construct a finite commutative group scheme G/k as follows: Let $\overline{G}$ be the constant group scheme over $\overline{k}$ whose group is isomorphic to M. Let σ act on $\overline{G}$ by permuting the points of $\overline{G}$ via the action of α, and extend this action by continuity to all of $\mathrm{Gal}(\overline{k}/k)$. Then let G be the group scheme obtained from $\overline{G}$ and this action of $\mathrm{Gal}(\overline{k}/k)$ by Weil descent. We briefly summarize this procedure by saying that G is the group scheme over k obtained from M by descending via the action of α.

Before we state the next proposition we need to introduce a duality on the category of finite R-modules. If M is a finite R-module, we let $\widehat{M}$ be the R-module that is equal to $\mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$ as an abelian group and where the actions of F and V are given by $(F\psi)(m) = \psi(Vm)$ and $(V\psi)(m) = \psi(Fm)$ for all $\psi \in \widehat{M}$ and all $m \in M$.

(4.14) **Proposition.** *Let notation be as above, and let M_{rr}, $M_{r\ell}$, and $M_{\ell r}$ be as in Lemma* 4.13. *Let G_{rr} (respectively, $G_{r\ell}$) be the group scheme over k obtained from M_{rr} (respectively, $M_{r\ell}$) by descending via the action of F, and let $G_{\ell r}$ be the Cartier dual of the group scheme over k obtained from $\widehat{M_{\ell r}}$ by descending via the action of F. Then* $\ker\mu$ *is isomorphic as a group scheme over k to the group scheme $G_{rr} \times G_{r\ell} \times G_{\ell r}$.*

Proof. Let $\overline{\mu}: \overline{C} \to \overline{D}$ be the isogeny of ordinary abelian varieties over $\overline{k}$ obtained from $\mu: C \to D$ by base extension. The arguments in [3, §§3 and 4] show that the kernel of $\overline{\mu}$ is isomorphic to the product of the constant group scheme $M_{rr} \oplus M_{r\ell}$ with the Cartier dual of the constant group scheme $\widehat{M_{\ell r}}$ over $\overline{k}$. Because μ is a k-isogeny, the Galois group $\mathrm{Gal}(\overline{k}/k)$ acts on the kernel of $\overline{\mu}$. On M_{rr} and $M_{r\ell}$, the action of $\mathrm{Gal}(\overline{k}/k)$ is simply the action defined by letting σ act as F, while on the Cartier dual of $\widehat{M_{\ell r}}$ the action is the dual of the action of $\mathrm{Gal}(\overline{k}/k)$ on $\widehat{M_{\ell r}}$ defined by letting σ act as F. Since taking duals commutes with descent, we get the proposition. □

(4.15) *Remark.* The group scheme G_{rr} is the *reduced-reduced* part of $\ker\mu$, that is, the largest factor of $\ker\mu$ that is reduced and that has a reduced dual. Likewise, $G_{r\ell}$ is the *reduced-local* part of $\ker\mu$, and $G_{\ell r}$ is the *local-reduced* part of $\ker\mu$.

(4.16) *Remark.* We end this section with an important observation: In the special case of the situation above when $B = \widehat{A}$ and $\lambda: A \to B$ is a polarization, there is a non-degenerate bilinear form e_λ from $\ker\lambda_{\mathbf{Q}/\mathbf{Z}}$ to $\mathbf{Q}/\mathbf{Z}$, defined by $e_\lambda(s/T_A, t/T_A) = \lambda_{\mathbf{Q}}(t)(s)/\mathbf{Z}$. If b is the semi-balanced form associated to λ, then $e_\lambda(s/T_A, t/T_A) = b_{\mathbf{Q}}(s, t)/\mathbf{Z}$, so e_λ is alternating and semi-balanced on the R-module $\ker\lambda_{\mathbf{Q}/\mathbf{Z}}$.

5. Kernels of polarizations of ordinary abelian varieties in a given isogeny class

Suppose $\mathscr{C}$ is an isogeny class of ordinary abelian varieties over a finite field k. We will call a finite group scheme G over k *attainable* in $\mathscr{C}$ if there is a polarization of a variety in $\mathscr{C}$ whose kernel is isomorphic to G. Similarly, if $\mathscr{C}$ is an isogeny class of Deligne modules and if M is a finite $R_{\mathscr{C}}$-module, we will call both M and its class in the Grothendieck group $G(R_{\mathscr{C}})$ *attainable* in

$\mathscr{C}$ if there is a polarization λ of a Deligne module in $\mathscr{C}$ such that $\ker \lambda_{\mathbf{Q}/\mathbf{Z}}$ is isomorphic as an $R_{\mathscr{C}}$-module to M. In this section we will prove Theorem 1.1, which describes up to Jordan-Hölder isomorphism the group schemes attainable in an isogeny class of ordinary abelian varieties. The results of §4 show that to prove this theorem it will be enough for us to prove the corresponding result for Deligne modules. This Deligne module result (Theorem 5.6 below) describes the elements of $G(R_{\mathscr{C}})$ that are attainable in a given isogeny class $\mathscr{C}$ of Deligne modules in terms of an obstruction group $\mathscr{B}(\mathscr{C})$ and a particular element $I_{\mathscr{C}}$ of that group. We begin by defining $\mathscr{B}(\mathscr{C})$ and $I_{\mathscr{C}}$.

If R is a CM-order, let $\mathscr{B}(R)$ be the cokernel of the norm map from $\mathrm{Ch}(R)$ to $\mathrm{Ch}^+(R^+)$. If $\psi: R \to S$ is a morphism of CM-orders, let ψ^+ be the induced map from R^+ to S^+. The map $\mathrm{Ch}^+(\psi^+)$ induces a map $\mathscr{B}(\psi)$ from $\mathscr{B}(S)$ to $\mathscr{B}(R)$, and $\mathscr{B}$ is a contravariant functor from the category of CM-orders to the category of abelian groups. We will usually write ψ^* for $\mathscr{B}(\psi)$. If $\mathscr{C}$ is an isogeny class of Deligne modules we define $\mathscr{B}(\mathscr{C})$ to be $\mathscr{B}(R_{\mathscr{C}})$. We will see in §10 that $\mathscr{B}(\mathscr{C})$ is a finite group annihilated by 2.

We will need a lemma in order to define the element $I_{\mathscr{C}}$.

(5.1) **Lemma.** *Let E be an algebraic number field with ring of integers A, let K be a quadratic extension of E, let B be the ring of integers of K, let $\mathfrak{d}_K$ be the different of $K/\mathbf{Q}$, and let σ be the non-trivial automorphism of K that fixes E. Suppose $x \in K$ satisfies $\sigma x = -x$. Then there is a fractional ideal $\mathfrak{a}$ of A such that $x\mathfrak{d}_K = \mathfrak{a}B$.*

Proof. Let $\mathfrak{d}_{K/E}$ be the relative different of K/E and let $\mathfrak{d}_E$ be the different of $E/\mathbf{Q}$, so that $\mathfrak{d}_K = \mathfrak{d}_{K/E}\mathfrak{d}_E$. Let $\Delta_{K/E}$ be the discriminant of K/E and let Δ_x be the discriminant of the A-lattice $A \oplus Ax$ in K. We know from [5, §3, Proposition 4(iii), p. 12] that $\Delta_x = 4x^2$, and part (i) of the same proposition tells us that there is a fractional ideal $\mathfrak{b}$ of A such that $\Delta_{K/E} = \mathfrak{b}^2\Delta_x = 4x^2\mathfrak{b}^2$. Since K/E is quadratic we have $\Delta_{K/E}B = \delta_{K/E}^2$, so multiplying the previous equality by x^2B gives $(x\delta_{K/E})^2 = (2x^2\mathfrak{b}B)^2$. Thus, $x\delta_{K/E} = 2x^2\mathfrak{b}B$ and $x\delta_K = 2x^2\mathfrak{b}\delta_E B$. Taking $\mathfrak{a} = 2x^2\mathfrak{b}\delta_E$, we are done. □

(5.2) **Definition.** Let K be a CM-field and Φ a CM-type of K. Let ι be a Φ-positive element of K and let $\mathfrak{d}$ be the different of $K/\mathbf{Q}$. By Lemma 5.1 there is a fractional ideal $\mathfrak{a}$ of K^+ that lifts to $\iota\mathfrak{d}$ in K, and we may write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ as a quotient of integral ideals of K^+. Define $I_{K,\Phi}$ to be the image of $[\mathscr{O}^+/\mathfrak{b}]_{\mathscr{O}^+} - [\mathscr{O}^+/\mathfrak{c}]_{\mathscr{O}^+}$ in $\mathscr{B}(\mathscr{O}_K)$. The element $I_{K,\Phi}$ does not depend on the choice of ι because the quotient of two Φ-positive numbers is a totally positive number, which becomes zero in $\mathrm{Ch}^+(\mathscr{O}^+)$.

(5.3) *Notation.* Let q be a power of a prime number p and choose an embedding $\varepsilon: W(\overline{\mathbf{F}}_q) \hookrightarrow \mathbf{C}$ of the ring of Witt vectors over $\overline{\mathbf{F}}_q$ into $\mathbf{C}$. If $\mathscr{C}$ is an isogeny class of Deligne q-modules, we write $\mathscr{C} = \prod_{i \in I} \mathscr{C}_i$ as a product of simple isogeny classes. We also write $\mathscr{C} = \prod_{j \in J} \mathscr{C}_j^{e_j}$ as a product of powers of distinct simple isogeny classes, where J is a subset of the index set I. Let $R = R_{\mathscr{C}}$, let $K = K_{\mathscr{C}}$, and let $\mathscr{O}$ be the integral closure of $\mathbf{Z}$ in K. For each $i \in I$ let $R_i = R_{\mathscr{C}_i}$, let $K_i = K_{\mathscr{C}_i}$, and let $\mathscr{O}_i$ be the ring of integers of K_i. Then $K = \prod_{j \in J} K_j$ and $\mathscr{O} = \prod_{j \in J} \mathscr{O}_j$, and the ring R is a subring of finite index in $\prod_{j \in J} R_j$. Each K_i is a CM-field. Our choice of the embedding ε

gives us a p-adic valuation on $\overline{\mathbf{Q}} \subset \mathbf{C}$, which, as in §4, gives us a CM-type Φ_i of K_i. For each $i \in I$ there is a unique $j \in J$ with $\mathscr{C}_i = \mathscr{C}_j$; let $\pi_i: R \to R_i$ be the composition of the projection $R \to R_j$ and the identification $R_j = R_i$, and let ρ_i be the composition of π_i and the inclusion $R_i \subset \mathscr{O}_i$.

(5.4) **Definition.** With notation as above, define $I_{\mathscr{C}}$ to be the element

$$\sum_{i \in I} \rho_i^*(I_{K_i, \Phi_i}) = \sum_{j \in J} e_j \rho_j^*(I_{K_j, \Phi_j})$$

of $\mathscr{B}(\mathscr{C})$.

It appears from the definition that $I_{\mathscr{C}}$ depends on our choice of the embedding ε, but we shall see in §11 that it does not.

(5.5) **Lemma.** *Let $\mathscr{C}$ be an isogeny class of Deligne modules. Then $R_{\mathscr{C}}$ is a free $R_{\mathscr{C}}^+$-module of rank two, generated by 1 and $F_{\mathscr{C}}$.*

Proof. This follows from the facts that $R_{\mathscr{C}} = R_{\mathscr{C}}^+[F_{\mathscr{C}}]$, that $F_{\mathscr{C}}$ is quadratic over $R_{\mathscr{C}}^+$, and that for every minimal prime $\mathfrak{p}$ of $R_{\mathscr{C}}$ the image of $F_{\mathscr{C}}$ in $R_{\mathscr{C}}/\mathfrak{p}$ is quadratic over the image of $R_{\mathscr{C}}^+$. □

In particular, if $R = R_{\mathscr{C}}$ then R is flat over R^+, so there is a tensoring map t_{R/R^+} from $G(R^+)$ to $G(R)$. This is the last fact that we need in order to state the main theorem.

(5.6) **Theorem.** *Let $\mathscr{C}$ be an isogeny class of Deligne modules, let $R = R_{\mathscr{C}}$, and let P be an element of $G(R)$. Then P is attainable if and only if $P = t_{R/R^+}(P')$ for some effective P' in $G(R_{\mathscr{C}}^+)$ whose image in $\mathscr{B}(\mathscr{C})$ is equal to $I_{\mathscr{C}}$. In particular, there is a principally polarized Deligne module in $\mathscr{C}$ if and only if $I_{\mathscr{C}} = 0$.*

To prove Theorem 5.6 we will need to use several propositions. We will state these propositions and some attendant definitions and comments in this section, but we will postpone the proofs of the propositions until later sections.

A simple Deligne module A is *maximal* if its endomorphism ring is the maximal order of K_A. Let $\mathscr{C}$ be a simple isogeny class of Deligne modules and let $R = R_{\mathscr{C}}$. An R-module M is *strongly attainable* in $\mathscr{C}$ if there is a maximal A in $\mathscr{C}$ and a polarization λ of A such that $\ker \lambda_{\mathbf{Q}/\mathbf{Z}}$ and M are isomorphic as R-modules. Maximal Deligne modules are particularly easy to study because their endomorphism rings are Dedekind domains, and kernels of polarizations of maximal Deligne modules are modules over Dedekind domains, as we shall see in §6. The first proposition we will need in the proof of Theorem 5.6 tells us exactly which R-modules are strongly attainable.

(5.7) **Proposition.** *Let $\mathscr{C}$ be a simple isogeny class of Deligne modules, let $R = R_{\mathscr{C}}$, let $K = K_{\mathscr{C}}$, let Φ be the CM-type of K obtained from the p-adic valuation v as in §4, and let $\mathscr{O} = \mathscr{O}_K$. Let M be a finite R-module. Then M is strongly attainable if and only if $M \cong_R \mathscr{O}/\mathfrak{a}\mathscr{O}$ for some ideal $\mathfrak{a}$ of $\mathscr{O}^+$ such that $\mathscr{O}^+/\mathfrak{a}$ maps to $I_{K,\Phi}$ in $\mathscr{B}(\mathscr{O})$.*

The next proposition tells us how we can obtain information about attainable $P \in G(R)$ from strongly attainable modules. It is at this point that we are forced to move to Jordan-Hölder isomorphism classes of modules.

(5.8) **Proposition.** *Let $\mathscr{C}$ be an isogeny class of Deligne modules and let notation be as in Notation 5.3. Let P be an element of $G(R)$. Then P is attainable if and only if P is effective and $P = Q + \overline{Q} + \sum_{i\in I}[M_i]_R$ for some $Q \in G(R)$ and some strongly attainable R_i-modules M_i.*

The last proposition we will need in the proof of Theorem 5.6 tells us that certain norm maps and tensor maps commute.

(5.9) **Proposition.** *Let $\mathscr{C}$ be an isogeny class of Deligne modules and let $R = R_{\mathscr{C}}$. Let $\mathfrak{p}$ be a minimal prime of R and let $\mathscr{O}$ be the integral closure of $R/\mathfrak{p}$ in its quotient ring. Then the diagram*

$$\begin{array}{ccc} G(\mathscr{O}) & \xleftarrow{t_{\mathscr{O}/\mathscr{O}^+}} & G(\mathscr{O}^+) \\ \downarrow & & \downarrow \\ G(R) & \xleftarrow{t_{R/R^+}} & G(R^+) \end{array}$$

commutes, where the vertical maps are the norms induced from the maps $R \to \mathscr{O}$ and $R^+ \to \mathscr{O}^+$.

Proof of Theorem 5.6. Let notation be as in Notation 5.3.

First we prove the "only if" part of the theorem. Assume $P \in G(R)$ is attainable. Then clearly P is effective. Also, by Proposition 5.8 we have $P = Q + \overline{Q} + \sum_{i\in I}[M_i]_R$ for some strongly attainable R_i-modules M_i and for some $Q \in G(R)$. By Proposition 5.7, for each i there is an ideal $\mathfrak{a}_i$ of $\mathscr{O}_i^+$ with $M_i \cong \mathscr{O}_i/\mathfrak{a}_i\mathscr{O}_i$ as R_i-modules and such that the image of $\mathscr{O}_i^+/\mathfrak{a}_i$ in $\mathscr{B}(\mathscr{O}_i)$ is I_{K_i,Φ_i}. Let Q_i be the image of $\mathscr{O}_i^+/\mathfrak{a}_i$ in $G(\mathscr{O}_i^+)$. Then by applying Proposition 5.9 we see that

$$\begin{aligned} P &= Q + \overline{Q} + \sum_{i\in I}[(\mathscr{O}_i^+/\mathfrak{a}_i) \otimes \mathscr{O}_i]_R \\ &= t_{R/R^+}(N_{R/R^+}(Q)) + \sum_{i\in I} t_{R/R^+}(N_{\mathscr{O}_i^+/R^+}(Q_i)). \end{aligned}$$

Let P' be the element $N_{R/R^+}(Q) + \sum_{i\in I} N_{\mathscr{O}_i^+/R^+}(Q_i)$ of $G(R^+)$. Then $P = t_{R/R^+}(P')$ and the image of P' in $\mathscr{B}(R)$ is equal to $\sum_{i\in I} \rho_i^*(I_{K_i,\Phi_i}) = I_{\mathscr{C}}$, as claimed. Also, P' must be effective since P is.

Next we prove the "if" part of the theorem. Suppose $P = t_{R/R^+}(P')$ for some effective $P' \in G(R^+)$ whose image in $\mathscr{B}(R)$ is $I_{\mathscr{C}}$. For each i let $\mathfrak{a}_i$ be an ideal of $\mathscr{O}_i^+$ such that $\mathscr{O}_i^+/\mathfrak{a}_i$ maps to I_{K_i,Φ_i} in $\mathscr{B}(\mathscr{O}_i)$. Since P' and $\sum_{i\in I}[\mathscr{O}_i^+/\mathfrak{a}_i]_{R^+}$ both map to $I_{\mathscr{C}}$ in $\mathscr{B}(R)$, there must be a $Q \in G(R)$ and a totally positive $x \in K^+$ such that

$$P' = N_{R/R^+}(Q) + \mathrm{Tr}_{R^+}(x) + \sum_{i\in I}[\mathscr{O}_i^+/\mathfrak{a}_i]_{R^+}.$$

In fact, we can choose Q and x so that $x \in R^+$. View x as an element of $\mathscr{O}^+$, and for each $j \in J$ let x_j be the jth component of x under the identification $\mathscr{O}^+ = \prod_{j\in J}\mathscr{O}_j^+$. For $i \in I \setminus J$ let $x_i = 1$. Since $Q(R^+) = Q(\mathscr{O}^+)$, by Lemma 2.1 we have $\mathrm{Tr}_{R^+} = N_{\mathscr{O}^+/R^+} \circ \mathrm{Tr}_{\mathscr{O}^+}$, which gives us

$$\mathrm{Tr}_{R^+}(x) = [\mathscr{O}^+/x\mathscr{O}^+]_{R^+} = \sum_{i\in I}[\mathscr{O}_i^+/x_i\mathscr{O}_i^+]_{R^+},$$

so that

$$P' = N_{R/R^+}(Q) + \sum_{i\in I}[\mathscr{O}_i^+/x_i\mathfrak{a}_i]_{R^+}.$$

For each i let $\mathfrak{b}_i$ be the ideal $x_i\mathfrak{a}_i$. The x_i are totally positive because x is, so for each i the image of $\mathscr{O}_i^+/\mathfrak{b}_i$ in $\mathscr{B}(\mathscr{O}_i)$ is I_{K_i,Φ_i}. By Proposition 5.9 we have

$$P = t_{R/R^+}(P') = Q + \overline{Q} + \sum_{i\in I}[\mathscr{O}_i/\mathfrak{b}_i\mathscr{O}_i]_R.$$

By Proposition 5.7 the R_i-modules $\mathscr{O}_i/\mathfrak{b}_i\mathscr{O}_i$ are strongly attainable, so P is attainable by Proposition 5.8.

The last sentence of the theorem is simply the special case when $P = 0$. □

We end this section by proving Theorem 1.1.

Proof of Theorem 1.1. Immediate from Theorem 5.6 upon applying the results of §4. □

6. Proof of Proposition 5.7

Let $\mathscr{C}$ be a simple isogeny class of Deligne modules, let $R = R_{\mathscr{C}}$, let K be the field $K_{\mathscr{C}}$, let Φ be the CM-type of K obtained from v, and let $\mathscr{O} = \mathscr{O}_K$. Let $^-$ denote the non-identity automorphism of K that fixes K^+. If $A = (T, F)$ is an element of $\mathscr{C}$, we can identify T with a lattice Λ in K that is a module over $R = \mathbf{Z}[F, V]$. Such an A is maximal if and only if Λ is actually a fractional $\mathscr{O}$-ideal in K.

Suppose A is maximal, corresponding as above to a fractional ideal $\mathfrak{a}$. Let $\mathfrak{b}$ be the conjugate (under $^-$) of the dual $\mathfrak{a}^\dagger$ of $\mathfrak{a}$ with respect to the trace $\mathrm{Tr}_{K/\mathbf{Q}}$ from K to $\mathbf{Q}$. If $\mathfrak{d}_K$ is the different of the field K we have $\mathfrak{a}^\dagger = \mathfrak{a}^{-1}\mathfrak{d}_K^{-1}$, so $\mathfrak{b} = \overline{\mathfrak{a}}^{-1}\mathfrak{d}_K^{-1}$ because $\overline{\mathfrak{d}_K} = \mathfrak{d}_K$. The lattice $\mathfrak{b}$ is also a module over R, and there is an R-semi-balanced perfect pairing $\mathfrak{a}\times\mathfrak{b} \to \mathbf{Z}$ given by $(x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\overline{y}x)$. From Definition 4.4, we see that the Deligne module determined by $\mathfrak{b}$ is the dual $\hat{A}$ of A.

Now, an isogeny from A to $\hat{A}$ is given by a non-zero $a \in K$ such that $a\mathfrak{a} \subset \mathfrak{b}$. Following §4, we define an R-semi-balanced form $b: \mathfrak{a}\times\mathfrak{a} \to \mathbf{Z}$ by taking $b(x, y) = \mathrm{Tr}_{K/\mathbf{Q}}(\overline{a}\overline{y}x)$. Let $S: K\times K \to K$ be the K-sesquilinear form given by $S(x, y) = \overline{a}\overline{y}x$, so that $b_{\mathbf{Q}} = \mathrm{Tr}_{K/\mathbf{Q}}\circ S$. For the isogeny given by a to be a polarization, the form S must satisfy the conditions of Definition 4.8, and we see from the definition of S that S will satisfy these conditions if and only if a is Φ-positive. Thus, polarizations of A correspond to Φ-positive $a \in K$ such that $a\mathfrak{a} \subset \overline{\mathfrak{a}}^{-1}\mathfrak{d}_K^{-1}$.

Suppose $a \in K$ gives a polarization λ of A. Then $\ker\lambda_{\mathbf{Q}/\mathbf{Z}}$ is isomorphic as an R-module to the $\mathscr{O}$-module $a^{-1}\overline{\mathfrak{a}}^{-1}\mathfrak{d}_K^{-1}/\mathfrak{a}$, which is isomorphic to $\mathscr{O}/(a\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{d}_K)$. By Lemma 5.1 there is a fractional ideal $\mathfrak{b}$ of $\mathscr{O}^+$ such that $a\mathfrak{d}_K = \mathfrak{b}\mathscr{O}$. Let $\mathfrak{c} = N_{\mathscr{O}/\mathscr{O}^+}(\mathfrak{a})\mathfrak{b}$. Then $\ker\lambda_{\mathbf{Q}/\mathbf{Z}} \cong \mathscr{O}/\mathfrak{c}\mathscr{O}$ and the image of $\mathscr{O}^+/\mathfrak{c}$ in $\mathscr{B}(\mathscr{O})$ is $I_{K,\Phi}$. Thus, all strongly attainable R-modules are of the form claimed in the proposition.

On the other hand, suppose $\mathfrak{c}$ is an integral $\mathscr{O}^+$-ideal such that the image of $\mathscr{O}^+/\mathfrak{c}$ in $\mathscr{B}(\mathscr{O})$ is $I_{K,\Phi}$. Then there must be a fractional ideal $\mathfrak{a}$ of $\mathscr{O}$ and a

Φ-positive $a \in K$ such that $c\mathscr{O} = a\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{d}_K$. If we let A be the maximal Deligne module corresponding to $\mathfrak{a} \subset K$ and if we let λ be the polarization of A given by a, then $\ker \lambda_{\mathbf{Q}/\mathbf{Z}} \cong_R \mathscr{O}/c\mathscr{O}$. □

7. Proof of Proposition 5.8

The proof of Proposition 5.8 is based on two other propositions. The first we state in some generality.

(7.1) **Proposition.** *Let R be a ring with an involution $^-$ and let M be an R-module such that $\#M < \infty$. Suppose b is a non-degenerate alternating semi-balanced form from M to $\mathbf{Q}/\mathbf{Z}$, and let P be an element of $G(R)$. Then there is an isotropic sub-R-module N of M such that $[\mathrm{Ann}_b(N)/N]_R = P$ if and only if $[M]_R \geq P \geq 0$ and there is a $Q \in G(R)$ with $[M]_R = P + Q + \bar{Q}$.*

To prove Proposition 7.1, we will need two lemmas.

(7.2) **Lemma.** *Let R be a ring with an involution $^-$ and let $p: L \times M \to N$ be a non-degenerate semi-balanced pairing from non-zero simple R-modules L and M to a group N. Then $L \cong \overline{M}$.*

Proof. If $\mathfrak{m}$ is the maximal ideal of R that kills M, then $\bar{\mathfrak{m}}$ kills L. □

(7.3) **Lemma.** *Let k be a finite field with an involution $^-$, let V be a k-vector space of dimension at least two, and let $b: V \times V \to \mathbf{Q}/\mathbf{Z}$ be an alternating semi-balanced form. Then there is a one-dimensional isotropic subspace W of V.*

Proof. We begin by noting that for any $x \in V$, to show that the subspace $k \cdot x$ is isotropic it suffices to check that $b(x, \alpha x) = 0$ for all $\alpha \in k$.

Suppose $^-$ is the identity map. Then we claim that *every* one-dimensional subspace of V is isotropic. We prove this first in the case that $\mathrm{char}(k) \neq 2$. Let x be any non-zero element of V and let $\alpha \in k$. Then

$$\begin{aligned} b(x, 2\alpha x) &= b(x, \alpha x) + b(x, \alpha x) \\ &= b(x, \alpha x) - b(\alpha x, x) \\ &= b(x, \alpha x) - b(x, \alpha x) = 0 \end{aligned}$$

where the second and the third equalities follow from that assumptions that b is alternating and semi-balanced, respectively. But every element of k is of the form 2α, so the one-dimensional subspace generated by x is isotropic. The case $\mathrm{char}(k) = 2$ is even simpler, because finite fields are perfect: Given any $\alpha \in k$, there is a $\beta \in k$ with $\alpha = \beta^2$, so that for every $x \in V$ we have

$$b(x, \alpha x) = b(x, \beta^2 x) = b(\beta x, \beta x) = 0$$

because b is alternating. Again we see that the subspace generated by x is isotropic.

Thus we can restrict our attention to the case where $^-$ is not the identity. Let k^+ be the fixed field of $^-$. Let W' be any one-dimensional subspace of

V. If $\mathrm{Ann}_b(W') \supset W'$ then W' is isotropic and we are done, so we need only consider the case where $\mathrm{Ann}_b(W') \cap W' = \{0\}$.

Pick any non-zero elements $x_0 \in W'$ and $x_1 \in \mathrm{Ann}_b(W')$, and for $i = 0, 1$ let $f_i: k \to \mathbf{Q}/\mathbf{Z}$ be defined by $f_i(\alpha) = b(\alpha x_i, x_i)$. For every $\alpha \in k^+$ there is a $\beta \in k$ with $\alpha = \beta\overline{\beta}$, because the norm map from k to k^+ is surjective. Therefore, for every $\alpha \in k^+$ we have

$$b(\alpha x_i, x_i) = b(\beta\overline{\beta}x_i, x_i) = b(\beta x_i, \beta x_i) = 0,$$

so f_0 and f_1 are non-zero elements of the k^+-vector space $\mathrm{Hom}(k/k^+, \mathbf{Q}/\mathbf{Z})$. But since k is finite, this is a one-dimensional k^+-vector space, so there is a $\gamma \in k^+$ such that $f_0 + f_1\gamma = 0$. Pick a $\delta \in k$ with $\gamma = \delta\overline{\delta}$, and let $x = x_0 + \delta x_1$. One can check that for all $\alpha \in k$ we have $b(\alpha x, x) = (f_0 + f_1\gamma)(\alpha) = 0$, so that $W = k \cdot x$ is a one-dimensional isotropic subspace of V. □

Proof of Proposition 7.1. Let ($\Rightarrow$) denote the "only if" part of the statement of the proposition, and let ($\Leftarrow$) denote the "if" part.

To prove ($\Rightarrow$), we note that taking the annihilators via b of a composition series for N gives a maximal sequence of R-modules lying between $\mathrm{Ann}_b(N)$ and M, and vice versa. The pairing b induces a non-degenerate semi-balanced pairing between each simple factor of N and the corresponding simple factor of $M/\mathrm{Ann}_b(N)$. By Lemma 7.2, the set of simple factors of $M/\mathrm{Ann}_b(N)$ is the set of conjugates (via $^-$) of the simple factors of N. Hence, if we let $Q = [N]_R$ then $[M]_R = [\mathrm{Ann}_b(N)/N] + [N]_R + [\overline{N}]_R = P + Q + \overline{Q}$, and furthermore, it is clear that $[M]_R \geq P \geq 0$.

We prove ($\Leftarrow$) by induction on the length of $[M]_R - P$. If $\mathrm{length}([M]_R - P) = 0$, then ($\Leftarrow$) is obviously true for this M and P; so assume $\mathrm{length}([M]_R - P) = m > 0$ and ($\Leftarrow$) holds for all R-modules M' and for all $P' \in G(R)$ such that the length of $[M']_R - P'$ is less than m.

Let S' be any non-zero simple R-module with $Q \geq [S']_R$ (such an S' exists because $2 \cdot \mathrm{length}(Q) = m > 0$). We claim that there is an isotropic sub-R-module S of M that is isomorphic to S'. We prove this as follows:

Let $\mathfrak{m} \subset R$ be the maximal ideal of R that annihilates S'. Since S' occurs in the composition series for M, the $\mathfrak{m}$-torsion T of M is non-zero. The module T is a vector space over the field $k = R/\mathfrak{m}$, which is finite because $\#M$ is finite.

If $\mathfrak{m} \neq \overline{\mathfrak{m}}$ then let S be any one-dimensional sub-k-vector space of T. By Lemma 7.2, the pairing $b|_{S \times S}$ must be trivial, so that S is an isotropic sub-R-module of M that is isomorphic to S'. We are left with the case when $\mathfrak{m} = \overline{\mathfrak{m}}$; in this case, the involution $^-$ induces an involution on k.

If $\dim_k(T) > 1$, then by Lemma 7.3 there is a one-dimensional isotropic subspace W of T, and we can take $S = W$. We are left with the case where $\dim_k(T) = 1$.

Let U be the $\mathfrak{m}$-power torsion of M and let $c = b|_{U \times U}$. We see that T is the unique minimal non-zero sub-R-module of U. Also, since $\mathfrak{m} = \overline{\mathfrak{m}}$ and since $[M]_R = P + Q + \overline{Q}$, the simple R-module k must occur at least twice in the list of composition factors of M; thus, we have $\mathrm{length}_R(U) \geq 2$, and in particular $T \neq U$. Since $T \neq U$, we have $\mathrm{Ann}_c(T) \neq 0$, so that $\mathrm{Ann}_c(T) \supset T$. Therefore, $S = T$ is an isotropic sub-R-module of M that is isomorphic to S', and we have proven our claim.

Let $M' = \mathrm{Ann}_b(S)/S$, and let b' be the non-degenerate alternating semi-balanced form on M' induced by b. Let $Q' = Q - [S]_R$; then $[M']_R = P + Q' + \overline{Q'}$, we have $[M']_R \geq P \geq 0$, and the length of $[M']_R - P$ is $m-2$, so we can apply the induction hypothesis to M' and P to find an isotropic sub-R-module N' of M' such that $[\mathrm{Ann}_{b'}(N')/N']_R = P$. Let N be the inverse image of N' under the reduction map from $\mathrm{Ann}_b(S)$ to M'. It is easy to check that the R-module N is isotropic and satisfies $[\mathrm{Ann}_b(N)/N]_R = P$. □

The second proposition we will use to prove Proposition 5.8 relates attainable modules to strongly attainable modules by showing that all polarizations can be obtained from diagonal polarizations of products of maximal Deligne modules. This proposition makes use of the pairing e_λ on the kernel of a polarization λ, defined in Remark 4.16.

(7.4) **Proposition.** *Let $\mathscr{C}$ be an isogeny class of Deligne modules and let notation be as in Notation* 5.3. *Let M be a finite R-module. Then M is attainable if and only if there are maximal Deligne modules A_i in $\mathscr{C}_i$ and polarizations λ_i of the A_i such that the R-module $\prod_{i\in I} \ker(\lambda_i \otimes (\mathbf{Q}/\mathbf{Z}))$ contains a sub-R-module N that is isotropic with respect to the pairing $e = \prod_{i\in I} e_{\lambda_i}$ and that satisfies $\mathrm{Ann}_e(N)/N \cong M$.*

Proof. First we prove the "if" direction. The proof will make no use of the assumption that the A_i are maximal.

Let $A = \prod_{i\in I} A_i$, let $\lambda = \prod_{i\in I} \lambda_i$, and write $A = (T, F)$. Let b be the R-semi-balanced form associated to λ and let S be the K-sesquilinear form associated to λ. Let U be the inverse image of N under the reduction map $\lambda_{\mathbf{Q}}^{-1}(\widehat{T}) \to \lambda_{\mathbf{Q}}^{-1}(\widehat{T})/T = \ker(\lambda \otimes (\mathbf{Q}/\mathbf{Z}))$, and let $B = (U, F)$. Using Remark 4.16 and the fact that N is isotropic, we see that

$$b_{\mathbf{Q}}(U, U)/\mathbf{Z} = e_\lambda(N, N) = 0/\mathbf{Z},$$

so if we let c be the form $b_{\mathbf{Q}}$ restricted to U, then c is an R-semi-balanced form from U to $\mathbf{Z}$. Let μ be the isogeny from B to $\widehat{B}$ associated to c. The sesquilinear form on $U_{\mathbf{Q}} = T_{\mathbf{Q}}$ associated to c is nothing other than S, and since we already know that S satisfies the conditions of Definition 4.8, the isogeny μ is a polarization.

The inclusion $T \subset U$ gives us an inclusion $\widehat{U} \subset \widehat{T}$, and since N is isotropic we have the sequence of inclusions $T \subset U \subset \lambda_{\mathbf{Q}}^{-1}(\widehat{U}) \subset \lambda_{\mathbf{Q}}^{-1}(\widehat{T})$. When we divide this sequence by T, we get $0 \subset N \subset \mathrm{Ann}_e(N) \subset \ker(\lambda \otimes (\mathbf{Q}/\mathbf{Z}))$, so we have

$$M \cong \mathrm{Ann}_e(N)/N \cong \lambda_{\mathbf{Q}}^{-1}(\widehat{U})/U = \mu_{\mathbf{Q}}^{-1}(\widehat{U})/U = \ker(\mu \otimes (\mathbf{Q}/\mathbf{Z})).$$

This shows that M is attainable.

To prove the "only if" direction, we choose a Deligne module $B = (U, F)$ in $\mathscr{C}$ and a polarization μ of B so that $M \cong \ker(\mu \otimes (\mathbf{Q}/\mathbf{Z}))$. Let c be the semi-balanced form associated to μ, and let S be the K-sesquilinear form on $U_{\mathbf{Q}}$ associated to μ. The decomposition of K into the product $\prod_{j\in J} K_j$ gives us a decomposition of $U_{\mathbf{Q}}$ into a product $\prod_{j\in J} U_j$, where each U_j is a vector

space over K_j of dimension e_j, where the e_j are as in Notation 5.3. By [17, Theorem 7.6.3, p. 259], we can find a basis for each U_j whose elements are pairwise orthogonal with respect to the sesquilinear form $S|_{U_j}$. The union of these bases is a set $\{x_i\}_{i\in I}$ that generates $U_{\mathbf{Q}}$ as a K-module, and the x_i are pairwise orthogonal under S. By reindexing the x_i if necessary, we can assume that for each $i \in I$, if j is the unique element of J such that $\mathscr{C}_i = \mathscr{C}_j$, then $K \cdot x_i = K_j \cdot x_i$, so that $K \cdot x_i$ is a one-dimensional vector space over $K_j = K_i$. By replacing the x_i by rational integer multiples, if necessary, we may assume that $\mathscr{O}_K \cdot x_i \subset U$. Let T be the sublattice $\sum_{i\in I} \mathscr{O}_K \cdot x_i$ of U, and for each $i \in I$ let $T_i = \mathscr{O}_K \cdot x_i$ and let F_i be the restriction of F to T_i. Let $A = (T, F)$ and for each i let $A_i = (T_i, F_i)$, so that $A = \prod_{i\in I} A_i$. For each i, the Deligne module A_i is in the isogeny class $\mathscr{C}_i$, and since its endomorphism ring is the ring of integers of K_i, it is maximal.

Since $T \subset U$, the image of $T\times T$ under c is contained in $\mathbf{Z}$. Let $b: T\times T \to \mathbf{Z}$ be the restriction of c to $T\times T$, and let λ be the polarization associated to b. For each $i \in I$ let b_i be the restriction of b to T_i, let $S_i: (T_i \otimes \mathbf{Q}) \times (T_i \otimes \mathbf{Q}) \to K_i$ be the associated sesquilinear form, and let $\lambda_i: A_i \to \widehat{A_i}$ be the associated isogeny. The form S on $T_{\mathbf{Q}}$ is the orthogonal sum of the S_i, so it is clear that the S_i satisfy the conditions of Definition 4.8. Thus, the λ_i are polarizations.

Finally, let N be the R-module U/T. When we divide the series of inclusions $T \subset U \subset \mu_{\mathbf{Q}}^{-1}(\widehat{U}) \subset \lambda_{\mathbf{Q}}^{-1}(\widehat{T})$ by T, we get $0 \subset N \subset \mathrm{Ann}_e(N) \subset \ker(\lambda \otimes (\mathbf{Q}/\mathbf{Z}))$. Thus N is an isotropic submodule of $\ker(\lambda \otimes (\mathbf{Q}/\mathbf{Z})) = \prod_{i\in I} \ker(\lambda_i \otimes (\mathbf{Q}/\mathbf{Z}))$ and $\mathrm{Ann}_e(N)/N \cong \mu_{\mathbf{Q}}^{-1}(\widehat{U})/U = \ker(\mu \otimes (\mathbf{Q}/\mathbf{Z})) \cong M$, so we are done. □

Proof of Proposition 5.8. First we prove the "only if" part of the proposition. Suppose $P \in G(R)$ is attainable, say $P = [L]_R$ for some attainable R-module L. Clearly P is effective. Also, by Proposition 7.4 there are strongly attainable R_i-modules M_i such that the R-module $M = \prod_{i\in I} M_i$ contains a sub-R-module N that is isotropic with respect to a non-degenerate alternating semi-linear form e on M and such that $\mathrm{Ann}_e(N)/N \cong_R L$. Then by Proposition 7.1 there must be a $Q \in G(R)$ such that $M = P + Q + \overline{Q}$. If we replace Q with $-Q$ we find that $P = Q + \overline{Q} + \sum_{i\in I}[M_i]_R$, as was to be shown.

Next we prove the "if" part of the proposition. Suppose $P \in G(R)$ is effective and there are strongly attainable R_i-modules M_i and a $Q \in G(R)$ with $P = Q + \overline{Q} + \sum_{i\in I}[M_i]_R$. For each i there is an $\mathscr{O}_i^+$-ideal $\mathfrak{a}_i$ such that $M_i \cong \mathscr{O}_i/\mathfrak{a}_i\mathscr{O}_i$.

Choose an $x \in \mathscr{O}$ such that $Q \le \mathrm{Pr}_R(x)$ and choose elements x_i of the $\mathscr{O}_i$ such that $[\mathscr{O}/x\mathscr{O}]_{\mathscr{O}} = \sum_{i\in I}[\mathscr{O}_i/x_i\mathscr{O}_i]_{\mathscr{O}}$. Replace Q with $Q - \mathrm{Pr}_R(x)$ and replace each M_i with $\mathscr{O}_i/x_i\overline{x}_i\mathfrak{a}_i\mathscr{O}_i$. Then we still have $P = Q + \overline{Q} + \sum_{i\in I}[M_i]_R$, and by Proposition 5.7 each M_i is still strongly attainable because $x_i\overline{x}_i$ is a totally positive element of $\mathscr{O}_i^+$. However, we also have $Q \le 0$, so that $P \le \sum_{i\in I}[M_i]_R$.

For each i pick a maximal $A_i \in \mathscr{C}_i$ and a polarization λ_i of A_i such that $M_i \cong \ker(\lambda_i \otimes (\mathbf{Q}/\mathbf{Z}))$. Let M be the R-module $\prod_{i\in I} M_i$ and let e be the non-degenerate R-semi-balanced pairing $\prod_{i\in I} e_{\lambda_i}$ from M to $\mathbf{Q}/\mathbf{Z}$. By Proposition 7.1 there is a sub-R-module N of M that is isotropic with respect to e and such that $[\mathrm{Ann}_e(N)/N]_R = P$. By Proposition 7.4, $\mathrm{Ann}_e(N)/N$ is attainable, so P is attainable. □

8. Proof of Proposition 5.9

To prove Proposition 5.9 we will need two lemmas.

(8.1) **Lemma.** *Suppose*

$$\begin{array}{ccc} D & \longleftarrow & C \\ \uparrow & & \uparrow \\ B & \longleftarrow & A \end{array}$$

is a commutative diagram of orders, where C is a Dedekind domain and where D and B are flat as modules over C and A, respectively. If the homomorphism $B \otimes_A C \to D$ obtained from this diagram is injective and if $B \otimes_A C$ has finite index in D, then the diagram

$$\begin{array}{ccc} G(D) & \xleftarrow{t_{D/C}} & G(C) \\ \downarrow{\scriptstyle N_{D/B}} & & \downarrow{\scriptstyle N_{C/A}} \\ G(B) & \xleftarrow{t_{B/A}} & G(A) \end{array}$$

commutes.

Proof. To check that the diagram commutes, we need only check that it commutes on the generators of $G(C)$, so suppose M is a simple C-module, say $M \cong C/\mathfrak{q}$ for some prime $\mathfrak{q}$ of C. Let $\mathfrak{p}$ be the contraction of $\mathfrak{q}$ to A. We must show that $[M \otimes_C D]_B = [M \otimes_A B]_B$, and to do this we may as well replace C and D with their localizations at the multiplicative set $C \setminus \mathfrak{q}$. This makes C a regular local ring, and we still have $B \otimes_A C \hookrightarrow D$ with finite index, because localization is exact.

Since C is a principal ideal domain, $M \cong C/\pi C$ for a prime element π of C, so that $M \otimes_C D = D/\pi D$ and $M \otimes_A B = (C \otimes_A B)/\pi(C \otimes_A B)$. Now consider the diagram of B-modules:

$$\begin{array}{ccc} D & \supset & \pi D \\ \cup & & \cup \\ C \otimes_A B & \supset & \pi(C \otimes_A B). \end{array}$$

Since $D/\pi(C \otimes_A B)$ is a finite B-module and since the two vertical quotient modules are isomorphic as B-modules, the two horizontal quotients must be Jordan-Hölder isomorphic as B-modules, which is precisely what we needed to show. □

(8.2) **Lemma.** *Let $\mathscr{C}$ be an isogeny class of Deligne modules and let $R = R_{\mathscr{C}}$. Let $\mathfrak{p}$ be a minimal prime of R and let $\mathscr{O}$ be the integral closure of $R/\mathfrak{p}$ in its quotient field. Then the homomorphism $R \otimes_{R^+} \mathscr{O}^+ \to \mathscr{O}$ obtained from the diagram*

$$\begin{array}{ccc} \mathscr{O} & \supset & \mathscr{O}^+ \\ \uparrow & & \uparrow \\ R & \supset & R^+ \end{array}$$

is injective, and the index of $R \otimes_{R^+} \mathscr{O}^+$ in $\mathscr{O}$ is finite.

Proof. The point here is that R is a free R^+-module of rank two generated by 1 and F, by Lemma 5.5. Thus, $R \otimes_{R^+} \mathscr{O}^+$ is a free rank two $\mathscr{O}^+$-module,

generated by $1 \otimes 1$ and $F \otimes 1$. Now, the image of $F \otimes 1$ in $\mathcal{O}$ is not contained in $\mathcal{O}^+$, because R is totally imaginary and $\mathcal{O}^+$ is totally real, and in fact 1 and the image of $F \otimes 1$ are linearly independent over $K^+ = \mathcal{O}^+ \otimes \mathbf{Q}$. Thus, $R \otimes_{R^+} \mathcal{O}^+$ injects into $\mathcal{O}$. Also, its image is the subring of $\mathcal{O}$ generated by $\mathcal{O}^+$ and the image of R, which is an order of $\mathcal{O}$ and which therefore has finite index in $\mathcal{O}$. □

Proof of Proposition 5.9. First we note that $\mathcal{O}$ is a flat $\mathcal{O}^+$-module and that R is a flat R^+-module, by Lemma 5.5. Then we simply apply Lemmas 8.2 and 8.1. □

9. The ring associated to an isogeny class

If we want to apply Theorem 5.6 to an actual isogeny class $\mathcal{C}$ of Deligne modules whose corresponding Weil polynomial h is given to us, we must somehow find a way to compute the group $\mathcal{B}(\mathcal{C})$ and the element $I_{\mathcal{C}}$ from the polynomial h. In §§10 and 11 we will show how we can calculate $\mathcal{B}(\mathcal{C})$ and $I_{\mathcal{C}}$ if we know enough about the rings $R_{\mathcal{C}}$ and $R^+_{\mathcal{C}}$. In particular, we will need to know about the singular primes of the ring $R_{\mathcal{C}}$ and about how the CM-fields that occur in the product of fields $K_{\mathcal{C}}$ ramify over their maximal real subfields. Thus it will be important for us to be able to calculate the discriminants of the $\mathbf{Z}$-algebras $R_{\mathcal{C}}$ and $R^+_{\mathcal{C}}$. In this section we will give formulas for these discriminants in terms of the coefficients of the polynomial h. The proofs of the results in this section are mainly computational; we will either omit them or give brief outlines.

Let $\mathcal{C}$ and h be as above. Let u be the *radical* of h, that is, the product of all of the monic $\mathbf{Q}$-irreducible factors of h, each taken once. The polynomial u is an ordinary Weil q-polynomial. Let $2n$ be the degree of u, and write $u = X^{2n} + b_{2n-1}X^{2n-1} + \cdots + b_1 X + b_0$. Let $R = R_{\mathcal{C}}$, let $F = F_{\mathcal{C}}$, let $V = V_{\mathcal{C}}$, and let K be the product of CM-fields $K_{\mathcal{C}}$.

(9.1) **Proposition.** *Let notation be as above and let* $\mathfrak{a}$ *be the ideal of* $A = \mathbf{Z}[X, Y]$ *generated by* r *and* s, *where* $r = XY - q$ *and where*

$$s = (X^n + Y^n) + b_{2n-1}(X^{n-1} + Y^{n-1}) + \cdots + b_{n+1}(X + Y) + b_n.$$

The ring homomorphism φ *from* A *to* R *that takes* X *to* F *and* Y *to* V *induces an isomorphism between* $A/\mathfrak{a}$ *and* R.

The proof is left to the reader.

(9.2) **Proposition.** *We have* $R^+ = \mathbf{Z}[F + V]$.

Again, the proof is left to the reader.

(9.3) *Remark.* For every integer $i \geq 0$ let T_i denote the ith Chebyshev polynomial, defined by $T_i(X) = \cos(i \cos^{-1} X)$. Let t_i denote the polynomial $2q^{i/2}T_i(X/2\sqrt{q})$. It is not hard to show that t_i has integer coefficients and that $F^i + V^i = t_i(F + V)$. Let s be the polynomial given in Proposition 9.1. It follows easily from the fact that $s(F, V) = 0$ that the minimal polynomial of $F + V$ is equal to

$$t = t_n + b_{2n-1}t_{n-1} + \cdots + b_{n+1}t_1 + b_n.$$

Thus, the order R^+ is isomorphic to the ring $\mathbf{Z}[X]/(t)$, and in particular the discriminant of R^+ is equal to the discriminant of the polynomial t.

(9.4) **Proposition.** *We have* $\Delta_R = (-1)^n \Delta_{R^+}^2 \cdot N_{K/\mathbf{Q}}(F - V)$.

Proof. We will only sketch a proof. The idea is that the ring R can be built up in two steps from the ring $\mathbf{Z}$: First one adjoins to $\mathbf{Z}$ a root of the monic polynomial t from Remark 9.3 to obtain R^+, and then one adjoins to R^+ a root of the monic polynomial $X^2 - (F + V)X + q$ to obtain R. One can show that the trace dual of R^+ with respect to $\mathbf{Z}$ is $(t'(F + V))^{-1}R^+$, where t' denotes the derivative of t. Similarly, the trace dual of R with respect to R^+ can be shown to be $(F - V)^{-1}R$. Thus the trace dual of R with respect to $\mathbf{Z}$ is $((F - V)t'(F + V))^{-1}R$. The absolute value of the discriminant of a $\mathbf{Z}$-algebra S is the index of S in its trace dual, so $|\Delta_R| = |\Delta_{R^+}|^2 \cdot |N_{K/\mathbf{Q}}(F - V)|$. If we keep track of the signs of the expressions in the last equality, we get the statement of the proposition. □

We are left with the task of calculating $N_{K/\mathbf{Q}}(F - V)$. The following proposition shows us how we may do this.

(9.5) **Proposition.** *In the above notation,*

$$N_{K/\mathbf{Q}}(F - V) = q^{-n}\left(\left(\sum_{0 \le i \le n} b_{2i} q^i\right)^2 - q\left(\sum_{0 \le i \le n-1} b_{2i+1} q^i\right)^2\right); \tag{2}$$

here $b_{2n} = 1$. *Furthermore, if* n *is even, say* $n = 2m$, *then*

$$N_{K/\mathbf{Q}}(F - V) = \left(b_n + 2\sum_{0 \le i < m} b_{2n-2i} q^{m-i}\right)^2 - q\left(2\sum_{0 \le i < m} b_{2n-(2i+1)} q^{m-(i+1)}\right)^2. \tag{3}$$

Proof. Let f be the minimal polynomial of F^2, so that $N_{K/\mathbf{Q}}(a - F^2) = f(a)$ for all $a \in \mathbf{Q}$. Since $\dim_{\mathbf{Q}} K$ is even we have $N_{K/\mathbf{Q}}(F^2 - q) = N_{K/\mathbf{Q}}(q - F^2)$, so we find that

$$N_{K/\mathbf{Q}}(F - V) = N_{K/\mathbf{Q}}(F^2 - q)/N_{K/\mathbf{Q}}(F) = f(q)/q^n.$$

If we write f in terms of the coefficients of the minimal polynomial u of F, we find that this last equality is equality (2). When n is even, the equality (3) follows from Proposition 3.4 and the equality (2). The verification of this last statement is left to the reader. □

We will use Propositions 9.4 and 9.5 in the examples of §§10 and 13.

10. Calculation of the obstruction group

Suppose $\mathscr{C}$ is an isogeny class of Deligne modules corresponding to an ordinary Weil polynomial h. In the previous section we gave a concrete description of the rings $R_{\mathscr{C}}$ and $R_{\mathscr{C}}^+$ in terms of the polynomial h, and we showed how one can calculate the discriminant of $R_{\mathscr{C}}$. Using this information, we can find the singular primes of $R_{\mathscr{C}}$. In this section we will show how knowledge of these singular primes and of the ramification behavior of the CM-fields occurring in $K_{\mathscr{C}}$ enables us to calculate the group $\mathscr{B}(\mathscr{C})$.

First we note in passing that if R is a CM-order that is locally free of rank 2 over R^+ then $\mathscr{B}(R)$ is a vector space over $\mathbf{F}_2$, because if S is a simple R^+-module then $[S \otimes R]_{R^+} = 2[S]_{R^+}$. For instance, $\mathscr{B}(R)$ is an $\mathbf{F}_2$-vector space

when R is the integral closure of $\mathbf{Z}$ in a product of CM-fields, and also when $R = R_{\mathscr{C}}$ for an isogeny class $\mathscr{C}$ of Deligne modules, by Lemma 5.5.

Our first proposition tells us how to calculate $\mathscr{B}(R)$ in the simplest possible case, when R is the ring of integers of a CM-field.

(10.1) **Proposition.** *Let $\mathscr{O}$ be the ring of integers of a CM-field K. Then*

$$\mathscr{B}(\mathscr{O}) \cong \begin{cases} 0 & \text{if } K/K^+ \text{ is ramified at a finite prime;} \\ \mathrm{Gal}(K/K^+) & \text{if not.} \end{cases}$$

In the second case, the isomorphism is provided by the Artin map.

Proof. Here we use the facts that $\mathrm{Ch}(\mathscr{O}) = \mathrm{Cl}(K)$ and $\mathrm{Ch}^+(\mathscr{O}^+) = \mathrm{Cl}^+(K^+)$, and the fact that the norm between the Chow groups corresponds to the ideal norm under this identification, to write $\mathscr{B}(\mathscr{O}) = \mathrm{Cl}^+(K^+)/N(\mathrm{Cl}(K))$.

Let L be the ray class field, modulo the infinite primes, of K^+; thus L is the maximal abelian extension of K^+ ramified at most at the infinite primes. Let M be the Hilbert class field of K, so that M is the maximal abelian extension of K that is unramified everywhere. Since L/K^+ is unramified at finite primes and since K/K^+ is ramified at all of the infinite primes, $K \cdot L$ is an unramified extension of K. It is also clearly abelian, so it is contained in M. The Artin map provides isomorphisms $\mathrm{Cl}^+(K^+) \cong \mathrm{Gal}(L/K^+)$ and $\mathrm{Cl}(K) \cong \mathrm{Gal}(M/K)$, and the restriction map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K^+)$ corresponds via these isomorphisms to the norm map on class groups.

If K/K^+ is ramified at a finite prime the extensions K/K^+ and L/K^+ are linearly disjoint, so that $\mathrm{Gal}(K \cdot L/K) \cong \mathrm{Gal}(L/K^+)$. In this case, the restriction map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(K \cdot L/K)$ is surjective, so the map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K^+)$ is surjective also. Thus, the norm map from $\mathrm{Cl}(K)$ to $\mathrm{Cl}^+(K^+)$ is surjective, and $\mathscr{B}(\mathscr{O}) \cong 0$.

On the other hand, if K/K^+ is unramified at all finite primes then K is contained in L. In this case, the image of $\mathrm{Gal}(M/K)$ under the restriction map to $\mathrm{Gal}(L/K^+)$ is equal to $\mathrm{Gal}(L/K)$, so that the cokernel of the restriction map is $\mathrm{Gal}(K/K^+) \cong \mathbf{Z}/2\mathbf{Z}$. □

(10.2) **Lemma.** *Let K be a CM-field and let g denote the degree of K^+ over $\mathbf{Q}$. If g is odd, then K/K^+ is ramified at a finite prime.*

Proof. We will prove the contrapositive statement. Suppose that K/K^+ is unramified at all finite primes. Let J be the idèle group of K^+ and let ψ be the idèlic Artin map from J to $\mathrm{Gal}(K/K^+)$. Then

$$\psi(-1) = \prod_{\mathfrak{p}|\infty} \psi_{\mathfrak{p}}(-1) \cdot \prod_{\mathfrak{p}<\infty} \psi_{\mathfrak{p}}(-1),$$

where the $\psi_{\mathfrak{p}}$ are the local Artin maps. Now for finite primes $\mathfrak{p}$ we have $\psi_{\mathfrak{p}}(-1) = 1$, because the finite primes are unramified in K/K^+ and because local Artin maps of unramified primes kill local units. For the infinite primes the local Artin maps are the sign function, and since the totally real field K^+ has g infinite primes, we see that $\psi(-1) = (-1)^g$. But the global Artin map ψ kills elements of $(K^+)^*$, so g must be even. □

(10.3) **Corollary.** *Let K be a CM-field and let g denote the degree of K^+ over $\mathbf{Q}$. If g is odd, then $\mathscr{B}(\mathscr{O}_K) \cong 0$.*

Proof. Immediate from Proposition 10.1 and Lemma 10.2. □

(10.4) **Proposition.** *Let S be a CM-order, and suppose R is a subring of finite index in S. Then*

$$\begin{array}{ccc} G(S^+)/N_{S/S^+}(G(S)) & \longrightarrow & \mathscr{B}(S) \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle i^*} \\ G(R^+)/N_{R/R^+}(G(R)) & \longrightarrow & \mathscr{B}(R) \end{array}$$

is a push-out diagram, where $i: R \to S$ is the inclusion map, where N is induced from the norm from $G(S^+)$ to $G(R^+)$, and where the horizontal maps are the natural reduction maps.

Proof. We start with the exact sequence

$$G(S) \xrightarrow{(N_{S/R}, -1)} G(R) \oplus G(S) \xrightarrow{1 \oplus N_{S/R}} G(R) \longrightarrow 0.$$

Let $K = Q(S)$. Then K is also $Q(R)$, because R is of finite index in S. From Lemma 2.1 we have $\mathrm{Pr}_R = N_{S/R} \circ \mathrm{Pr}_S$, and by dividing the last two terms of the preceding sequence by the image of K^* under Pr_S and Pr_R we see that the sequence

$$(4) \qquad G(S) \xrightarrow{(N_{S/R}, -\chi)} G(R) \oplus \mathrm{Ch}(S) \xrightarrow{\psi \oplus \mathrm{Ch}(i)} \mathrm{Ch}(R) \longrightarrow 0$$

is exact, where $\psi: G(R) \to \mathrm{Ch}(R)$ and $\chi: G(S) \to \mathrm{Ch}(S)$ are the natural reduction maps. In a similar manner we get an exact sequence

$$(5) \qquad G(S^+) \longrightarrow G(R^+) \oplus \mathrm{Ch}^+(S^+) \longrightarrow \mathrm{Ch}^+(R^+) \longrightarrow 0,$$

and taking the cokernel of the norm map from (4) to (5) gives us the exact sequence

(6)

$$G(S^+)/N(G(S)) \xrightarrow{(N, -\chi)} \big(G(R^+)/N(G(R))\big) \oplus \mathscr{B}(S) \xrightarrow{\psi \oplus i^*} \mathscr{B}(R) \longrightarrow 0.$$

This sequence being exact is exactly what it means for the diagram of the proposition to be a push-out diagram. □

The two groups on the left-hand side of the diagram of Proposition 10.4 are infinite. It is possible to replace them with finite groups; we will show how to do this in a special case that will be enough for our purposes.

Suppose S is a CM-order, R is a subring of finite index in S, and R and S are locally free of rank 2 over R^+ and S^+. Let $C = G(R^+)/N_{R/R^+}(G(R))$ and let $D = G(S^+)/N_{S/S^+}(G(S))$; our assumptions on R and S imply that the groups C and D are vector spaces over $\mathbf{F}_2$.

Let $\mathfrak{p}$ be a maximal ideal of R^+. Then $[R^+/\mathfrak{p}]_{R^+}$ is not in the image of the norm from $G(R)$ if and only if $\mathfrak{p}$ is inert in R/R^+. Let X be the set of maximal $\mathfrak{p}$ of R^+ that are inert in R/R^+, and let Y be the set of maximal $\mathfrak{q}$ of S^+ that are inert in S/S^+. For each $\mathfrak{p}$ in X let $x_\mathfrak{p}$ be the image of $[R^+/\mathfrak{p}]_{R^+}$ in C, and for each $\mathfrak{q}$ in Y let $y_\mathfrak{q}$ be the image of $[S^+/\mathfrak{q}]_{S^+}$ in D. Then the $x_\mathfrak{p}$ form a basis for C as an $\mathbf{F}_2$-vector space, as do the $y_\mathfrak{q}$ for D. Suppose $\mathfrak{q} \in Y$, and let $\mathfrak{p} = \mathfrak{q} \cap R^+$. If $\mathfrak{p}$ is not in X, or if the residue field $k(\mathfrak{q})$ of $\mathfrak{q}$ is of even degree over the residue field $k(\mathfrak{p})$, then the norm from D to C of $y_\mathfrak{q}$ is zero, while if $[k(\mathfrak{q}): k(\mathfrak{p})]$ is odd and $\mathfrak{p}$ is in X, then $N(y_\mathfrak{q}) = x_\mathfrak{p} \neq 0$.

Let X_{ns} be the set of $\mathfrak{p}$ in X that are non-singular, that is, those $\mathfrak{p}$ in X whose local rings are regular local rings. Let Y_{ns} be the set of $\mathfrak{q}$ in Y that lie over some $\mathfrak{p}$ in X_{ns}. Let C_{ns} be the subspace of C spanned by $\{x_{\mathfrak{p}} \mid \mathfrak{p} \in X_{ns}\}$, let C_s be the subspace of C spanned by $\{x_{\mathfrak{p}} \mid \mathfrak{p} \in X \setminus X_{ns}\}$, let D_{ns} be the subspace of D spanned by $\{y_{\mathfrak{q}} \mid \mathfrak{q} \in Y_{ns}\}$, and let D_s be the subspace of D spanned by $\{y_{\mathfrak{q}} \mid \mathfrak{q} \in Y \setminus Y_{ns}\}$. We see that C_s and D_s are finite-dimensional, that $C = C_s \oplus C_{ns}$, that $D = D_s \oplus D_{ns}$, and that the norm $N: D \to C$ takes D_s to C_s and D_{ns} to C_{ns}.

(10.5) **Proposition.** *Let notation be as above. The diagram*

$$\begin{array}{ccc} D_s & \longrightarrow & \mathscr{B}(S) \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle i^*} \\ C_s & \longrightarrow & \mathscr{B}(R) \end{array}$$

is a push-out diagram, where the horizontal maps are the restrictions to D_s and C_s of the natural reduction maps.

Proof. Suppose we can show that the norm N gives an isomorphism between D_{ns} and C_{ns}. Then a simple diagram chase applied to the natural map from the sequence (6) to the sequence

$$D_s \longrightarrow C_s \oplus \mathscr{B}(S) \longrightarrow \mathscr{B}(R) \longrightarrow 0$$

shows that the latter sequence is exact, which is what we want.

In order to show that N gives an isomorphism between D_{ns} and C_{ns}, we must show that for every $\mathfrak{p}$ in X_{ns} there is exactly one $\mathfrak{q}$ in Y_{ns} lying over it, and that the degree of $k(\mathfrak{q})$ over $k(\mathfrak{p})$ is odd. To accomplish this, we will show first that there is exactly one prime $\mathfrak{q}$ of S^+ lying over $\mathfrak{p}$, second that $k(\mathfrak{q}) = k(\mathfrak{p})$, and third that $\mathfrak{q}$ is inert in S/S^+.

Let $\mathfrak{p}$ be an element of X_{ns} and let $R^+_{\mathfrak{p}}$ be the localization of R^+ at $\mathfrak{p}$. Then $R^+_{\mathfrak{p}}$ is of finite index in $S^+ \otimes_{R^+} R^+_{\mathfrak{p}}$, and since $R^+_{\mathfrak{p}}$ is a discrete valuation ring we must have $S^+ \otimes_{R^+} R^+_{\mathfrak{p}} = R^+_{\mathfrak{p}}$. Thus, S^+ has exactly one prime $\mathfrak{q}$ lying over $\mathfrak{p}$, and since $S^+_{\mathfrak{q}} = R^+_{\mathfrak{p}}$, the residue fields of $\mathfrak{q}$ and $\mathfrak{p}$ are equal.

Let $\mathfrak{q}'$ be any prime of S lying over $\mathfrak{q}$. Then $\mathfrak{q}' \cap R = \mathfrak{p}'$ is the prime of R lying over $\mathfrak{p}$, and the residue fields of these various primes satisfy $k(\mathfrak{q}') \supset k(\mathfrak{p}') \supset k(\mathfrak{p}) = k(\mathfrak{q})$. Since $\mathfrak{p}$ is inert in R/R^+, the second containment is strict, and $\mathfrak{q}$ must be inert in S/S^+. □

(10.6) *Remark.* It will be useful in our examples to have a description of the vector space D_s other than its definition. We will give such an alternate description by giving a characterization of the primes in the set $Y \setminus Y_{ns}$. Suppose $\mathfrak{q}$ is a prime of S^+ that is in Y, and let $\mathfrak{p}$ be the prime $\mathfrak{q} \cap R^+$ of R^+. To say that $\mathfrak{q}$ is not in Y_{ns} means exactly that $\mathfrak{p}$ is not in X_{ns}, and this means that either $\mathfrak{p}$ is not in X or $\mathfrak{p}$ is in X but is singular. In the first case, $\mathfrak{p}$ is not inert in R/R^+, and the fact that $\mathfrak{q}$ is inert in S/S^+ implies that $\mathfrak{p}$ lies under a singular prime of R. In the second case, every prime of R lying over $\mathfrak{p}$ is singular. Conversely, if $\mathfrak{p}$ lies under a singular prime of R then either $\mathfrak{p}$ is not inert in R/R^+ or $\mathfrak{p}$ is in $X \setminus X_{ns}$. Thus, the set $Y \setminus Y_{ns}$ consists of those primes of S^+ that are inert in S/S^+ and whose restrictions to R^+ lie under singular primes of R.

We can use Propositions 10.5 and 10.1, along with the trivial observation that $\mathscr{B}(\prod R_i) = \bigoplus \mathscr{B}(R_i)$, to compute $\mathscr{B}(\mathscr{C})$ for isogeny classes $\mathscr{C}$ of Deligne modules. Suppose $\mathscr{C}$ is an isogeny class of Deligne modules, write $\mathscr{C} = \prod_{j\in J} \mathscr{C}_j^{e_j}$ as a product of powers of distinct simple isogeny classes, and let notation be as in Notation 5.3, so that K is isomorphic to the product of the fields K_j, the ring $\mathscr{O}$ is isomorphic to the product of the $\mathscr{O}_j$, and R is isomorphic to a subring of the product of the R_j. There are two ways to proceed. One way is to calculate $\mathscr{B}(\mathscr{O})$ as the direct sum of the $\mathscr{B}(\mathscr{O}_j)$, which we can compute from Proposition 10.1, and then to use Proposition 10.5 applied to the inclusion $R \subset \mathscr{O}$ to calculate $\mathscr{B}(R)$. Our other option is to calculate the $\mathscr{B}(R_j)$ from Proposition 10.5 applied to the inclusions $R_j \subset \mathscr{O}_j$, and then to use the same proposition on the inclusion $R \subset \prod_{j\in J} R_j$ to find $\mathscr{B}(R)$.

We end this section by demonstrating the use of Proposition 10.5 in two examples. In both examples we maintain the notation used in Proposition 10.5 and in the discussion preceding it.

(10.7) **Example: Ordinary elliptic curves.** Let $\mathscr{C}$ be an isogeny class of ordinary elliptic curves over a finite field, let $R = R_{\mathscr{C}}$, let $K = K_{\mathscr{C}}$, and let $\mathscr{O} = \mathscr{O}_K$. We will apply Proposition 10.5 with $S = \mathscr{O}$. The CM-field K is an imaginary quadratic extension of $\mathbf{Q}$, and from Corollary 10.3 we see that $\mathscr{B}(\mathscr{O}) \cong 0$. The ring R is an order in K, and $R^+ = \mathbf{Z}$. Every prime of $\mathbf{Z}$ is regular, so $X \setminus X_{\mathrm{ns}}$ is empty and $C_{\mathrm{s}} = 0$. From Proposition 10.5, we see that $\mathscr{B}(R) = 0$.

(10.8) **Example.** Let $p = 197$ and let f be the polynomial $X^4 + X^3 + X^2 + pX + p^2$. One can check that f is an ordinary Weil p-polynomial; for instance, see [16]. Let $K = \mathbf{Q}[X]/(f)$ and let π be the image of X in K, so that $K = K_{\mathscr{C}}$ for the isogeny class $\mathscr{C}$ of Deligne modules associated to f, and $R_{\mathscr{C}} = \mathbf{Z}[\pi, \overline{\pi}]$. Let $\mathscr{O} = \mathscr{O}_K$. We will apply Proposition 10.5 with $S = \mathscr{O}$.

The minimal polynomial g of $\pi+\overline{\pi}$ is $X^2+X+(1-2p)$ and the discriminant of g is $1573 = 11^2 \cdot 13$, so $K^+ \cong \mathbf{Q}(\sqrt{13})$. The narrow class number of K^+ is one, so K/K^+ must be ramified at some finite prime. Proposition 10.1 tells us that $\mathscr{B}(\mathscr{O}) \cong 0$.

The discriminant Δ_{R^+} of R^+, which is the discriminant of the polynomial g, differs from the discriminant $\Delta_{\mathscr{O}^+}$ of $\mathscr{O}^+$ by the factor 11^2, so the singular primes of R^+ lie over 11. In fact R^+ has exactly one prime $\mathfrak{p}$ over 11, the prime $\mathfrak{p}$ is singular, and the residue field of $\mathfrak{p}$ is $\mathbf{F}_{11}$. Since f factors modulo 11 as the square of the irreducible polynomial $X^2+6X-1 \pmod{11}$, the prime $\mathfrak{p}$ is inert in R/R^+. Thus, $X \setminus X_{\mathrm{ns}} = \{\mathfrak{p}\}$ and $C_{\mathrm{s}} \cong \mathbf{F}_2$.

One can check, using Proposition 9.5 for instance, that the norm from K to $\mathbf{Q}$ of $\pi - \overline{\pi}$ is $29 \cdot 53 \cdot 101$, so by Proposition 9.4 the discriminant Δ_R of R is $11^4 \cdot 13^2 \cdot 29 \cdot 53 \cdot 101$. The quotient of Δ_R by the discriminant $\Delta_{\mathscr{O}}$ of $\mathscr{O}$ is a square, and since $\Delta_{\mathscr{O}}$ is divisible by $\Delta_{\mathscr{O}^+}^2 = 13^2$ the quotient $\Delta_R/\Delta_{\mathscr{O}}$ must be a divisor of 11^4. Thus, all of the singular primes of R lie over 11, so by Remark 10.6 the set $Y \setminus Y_{\mathrm{ns}}$ consists of those primes of $\mathscr{O}^+$ that are inert in $\mathscr{O}/\mathscr{O}^+$ and that lie over 11. Now, $\mathscr{O}^+$ has one prime $\mathfrak{q}$ over 11, with residue field $\mathbf{F}_{121}$, and because f factors modulo 11 as the square of an irreducible quadratic polynomial, $\mathfrak{q}$ is not inert in $\mathscr{O}/\mathscr{O}^+$. Thus, $Y \setminus Y_{\mathrm{ns}}$ is empty and $D_{\mathrm{s}} = 0$. Proposition 10.5 tells us that $\mathscr{B}(R) \cong \mathbf{F}_2$. This example shows that it is possible for $\mathscr{B}(\mathscr{C})$ to be non-zero when $\mathscr{B}(\mathscr{O})$ is zero.

11. Calculation of the obstruction element

Our task in this section is to show how one may calculate the element $I_{\mathscr{C}}$ of $\mathscr{B}(\mathscr{C})$ for an isogeny class $\mathscr{C}$ of Deligne modules. Given an isogeny class $\mathscr{C}$, we can write $\mathscr{C} = \prod_{j\in J} \mathscr{C}_j^{e_j}$ as a product of powers of distinct simple isogeny classes. Using the results of the previous section, we can calculate the group $\mathscr{B}(\mathscr{C})$, the groups $\mathscr{B}(\mathscr{C}_j)$, and the homomorphisms $\pi_j^*: \mathscr{B}(\mathscr{C}_j) \to \mathscr{B}(\mathscr{C})$ obtained from the homomorphisms $\pi_j: R_{\mathscr{C}} \to R_{\mathscr{C}_j}$ defined in Notation 5.3. It follows from Definition 5.4 and the functoriality of $\mathscr{B}$ that $I_{\mathscr{C}} = \sum e_j \pi_j^*(I_{\mathscr{C}_j})$, so it will be enough for us in this section to show how one may calculate $I_{\mathscr{C}}$ for simple isogeny classes $\mathscr{C}$. To start with, we will show how to calculate the element $I_{K,\Phi}$ of $\mathscr{B}(\mathscr{O}_K)$ for a CM-field K with CM-type Φ (see Definition 5.2).

Suppose K is a CM-field and Φ is a CM-type of K. We define the *Φ-norm* to be the map $N_\Phi: K \to \mathbf{C}$ given by $N_\Phi(x) = \prod_{\varphi\in\Phi} \varphi(x)$. Notice that $N_\Phi(x)\overline{N_\Phi(x)} = N_{K/\mathbf{Q}}(x)$ for all $x \in K$. If ρ is the non-trivial automorphism of K that fixes K^+, we let $K^\#$ be the subgroup $\{x \in K^* : \rho(x) = \pm x\}$ of K^*; the group $K^\#$ consists of the elements of K^* that are either totally real or totally imaginary. Suppose K/K^+ is unramified at all finite primes; then by Lemma 10.2 the degree g of K^+ over $\mathbf{Q}$ is even, and we define a map $\chi_{K,\Phi}: K^\# \to \mathrm{Gal}(K/K^+)$ as follows: If $x \in K^\#$ then the fractional ideal (x) of $\mathscr{O}_K$ is fixed by ρ and so may be viewed as a fractional ideal of $\mathscr{O}_{K^+}$. Identify $\mathrm{Gal}(K/K^+)$ with the group $\{\pm 1\}$ and define $\chi_{K,\Phi}(x)$ to be $\mathrm{sign}(N_\Phi(x)) \cdot ((x), K/K^+)$; here $(\,\cdot\,, K/K^+)$ is the Artin map. The sign of $N_\Phi(x)$ is meaningful because $N_\Phi(x)$ is real for $x \in K^\#$ when g is even. If $x \in K^\#$ is totally real, then $\mathrm{sign}(N_\Phi(x)) = \prod_{\varphi\in\Phi} \mathrm{sign}(\varphi(x))$, so that $\chi_{K,\Phi}(x)$ is the idèlic Artin map evaluated on the principal idèle x. Since the idèlic Artin map kills principal idèles, we see that $\chi_{K,\Phi}(x) = 1$ for all totally real $x \in K^\#$. Thus $\chi_{K,\Phi}$ induces a homomorphism $X_{K,\Phi}$ from the group $K^\#/(K^+)^* \cong \{\pm 1\}$ to the group $\mathrm{Gal}(K/K^+) \cong \{\pm 1\}$; the homomorphism $X_{K,\Phi}$ is either 1 or -1 under the identification $\mathrm{Hom}(\{\pm 1\}, \{\pm 1\}) \cong \{\pm 1\}$.

(11.1) **Proposition.** *Let K be a CM-field with ring of integers $\mathscr{O}$ and let Φ be a CM-type of K. If K/K^+ is ramified at any finite prime, then $I_{K,\Phi} = 0$. If K/K^+ is unramified at all finite primes, then $[K^+ : \mathbf{Q}]$ is even, and $I_{K,\Phi} = 0$ if and only if $X_{K,\Phi} = 1$.*

Proof. If K/K^+ is ramified at a finite prime, then by Proposition 10.1 the group $\mathscr{B}(\mathscr{O})$ is trivial and $I_{K,\Phi}$ must be 0. So let us assume for the rest of the proof that K/K^+ is unramified at all finite primes. By Lemma 10.2, the degree $g = [K^+ : \mathbf{Q}]$ is even. Let $\mathfrak{d}$ be the different of $K/\mathbf{Q}$ and let $\mathfrak{d}'$ be the different of $K^+/\mathbf{Q}$. Since K/K^+ is unramified at finite primes, $\mathfrak{d} = \mathfrak{d}'\mathscr{O}$. Let ι be a Φ-positive element of K, and let $\mathfrak{a}$ be the fractional ideal of $\mathscr{O}^+$ such that $(\iota) = \mathfrak{a}\mathscr{O}$. By Definition 5.2, the element $I_{K,\Phi}$ of $\mathscr{B}(\mathscr{O})$ is equal to the image of $\mathfrak{a}\mathfrak{d}'$ in $\mathscr{B}(\mathscr{O})$, and the image of $I_{K,\Phi}$ under the isomorphism $\mathscr{B}(\mathscr{O}) \cong \mathrm{Gal}(K/K^+)$ of Proposition 10.1 is equal to the Artin symbol $(\mathfrak{a}\mathfrak{d}', K/K^+) = (\mathfrak{a}, K/K^+)(\mathfrak{d}', K/K^+)$. But by [2, Theorem 3, p. 241] we have $(\mathfrak{d}', K/K^+) = (-1)^{g/2}$, and since ι is Φ-positive this is equal to the sign of $N_\Phi(\iota)$. Thus $(\mathfrak{a}\mathfrak{d}', K/K^+) = \chi_{K,\Phi}(\iota)$, so that $I_{K,\Phi} = 0$ if and only if $\chi_{K,\Phi}(\iota) = 1$, which in turn holds if and only if $X_{K,\Phi} = 1$. □

Now let $\mathscr{C}$ be an isogeny class of simple Deligne modules. As usual, let $R = R_{\mathscr{C}} = \mathbf{Z}[F, V]$, let $K = K_{\mathscr{C}}$, let $\mathscr{O} = \mathscr{O}_K$, and let i be the natural inclusion $R \to \mathscr{O}$. Let v be the p-adic valuation on $\overline{\mathbf{Q}} \subset \mathbf{C}$ obtained from the embedding $\varepsilon: W \hookrightarrow \mathbf{C}$ we chose in §5, and let Φ be the CM-type

$$\Phi = \{\varphi: K \to \mathbf{C} \mid v(\varphi(F)) > 0\}$$

obtained from v. By Definition 5.4, the element $I_{\mathscr{C}}$ of $\mathscr{B}(\mathscr{C})$ is equal to $i^*(I_{K,\Phi})$. This definition makes it appear as though $I_{\mathscr{C}}$ depends on the p-adic valuation v that gives us Φ. The next proposition shows that this is not the case.

(11.2) **Proposition.** *Let notation be as above and let v' be any p-adic valuation on $\overline{\mathbf{Q}} \subset \mathbf{C}$, not necessarily equal to v. Let Φ' be the CM-type*

$$\Phi' = \{\varphi: K \to \mathbf{C} \mid v'(\varphi(F)) > 0\}$$

of K. Then $I_{K,\Phi'} = I_{K,\Phi}$.

Proof. If K/K^+ is ramified at a finite prime, then $I_{K,\Phi}$ and $I_{K,\Phi'}$ are both equal to 0, so we are left with the case when K/K^+ is unramified at all finite primes. Let $x \in K^*$ be totally imaginary. For $\Psi = \Phi, \Phi'$ we have that $I_{K,\Psi} = 0$ if and only if $X_{K,\Psi} = 1$, which in turn holds if and only if

$$1 = \chi_{K,\Psi}(x) = \operatorname{sign}(N_\Psi(x)) \cdot ((x), K/K^+).$$

Thus, to show that $I_{K,\Phi} = I_{K,\Phi'}$ we have only to show that $N_\Phi(x)$ and $N_{\Phi'}(x)$ have the same sign. In fact, we will show that $N_\Phi(x) = N_{\Phi'}(x)$, and that these numbers are in $\mathbf{Q}$.

We have already noted that $N_\Phi(x)\overline{N_\Phi(x)} = N_{K/\mathbf{Q}}(x)$, and since g is even we have $N_\Phi(x) \in \mathbf{R}$, so that $N_{K/\mathbf{Q}}(x) = (N_\Phi(x))^2$. Also, the ideal $(N_{K/\mathbf{Q}}(x))$ is equal to the norm from K to $\mathbf{Q}$ of the ideal (x) of K, and since (x) is the lift to K of an ideal $\mathfrak{a}$ of K^+, we have that $(N_{K/\mathbf{Q}}(x)) = (N_{K^+/\mathbf{Q}}(\mathfrak{a}))^2$ is a square of an ideal of $\mathbf{Q}$. Hence, $N_\Phi(x) \in \mathbf{Q}$.

Now, $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts transitively on the p-adic valuations of $\overline{\mathbf{Q}}$, so there is a $\sigma \in \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $v' = v\sigma$. From this we see that $\Phi' = \sigma^{-1}\Phi$, from which we deduce that $N_{\Phi'}(x) = \sigma^{-1}(N_\Phi(x))$. Since $N_\Phi(x) \in \mathbf{Q}$, we have $N_{\Phi'}(x) = N_\Phi(x)$. □

We have already noted that for our simple isogeny class $\mathscr{C}$ of Deligne modules we have $I_{\mathscr{C}} = i^*(I_{K,\Phi})$, where $i: R \to \mathscr{O}$ is the inclusion map and notation is as above. Our next proposition tells us when i^* is the zero map.

(11.3) **Proposition.** *Let $\mathscr{C}$ be a simple isogeny class of g-dimensional Deligne modules and let notation be as above. If K/K^+ is ramified at a finite prime, or if there is a prime $\mathfrak{q}$ of K^+ that divides $(F - V)$ and that is inert in K/K^+, then i^* is the zero map and $I_{\mathscr{C}} = 0$. Otherwise, g is even, i^* is not the zero map, and $I_{\mathscr{C}} = 0$ if and only if $N_\Phi(F - V) > 0$.*

Proof. If K/K^+ is ramified at a finite prime, then from Proposition 10.1 we know that $\mathscr{B}(\mathscr{O}) = 0$, so that i^* must be the zero map. So assume that K/K^+ is unramified at every finite prime. In this case $\mathscr{B}(\mathscr{O}) \cong \mathbf{Z}/2\mathbf{Z}$, and by Lemma 10.2 the dimension g is even. We will show that the map i^* is the zero map if and only if there is a $\mathfrak{q}$ of K^+ that divides $F - V$ and that is inert in K/K^+.

Let z be the non-zero element of $\mathscr{B}(\mathscr{O})$, and adopt the notation preceding Proposition 10.5, with $S = \mathscr{O}$. Suppose $i^*(z) = 0$. Then by Proposition 10.5 there must be a $y \in D_S$ that maps to z in $\mathscr{B}(\mathscr{O})$ and that maps to 0 in C_S. Since the basis elements $y_\mathfrak{q}$ of D_S all map to z in $\mathscr{B}(\mathscr{O})$, and since each $y_\mathfrak{q}$ maps either to 0 or to one of the basis elements $x_\mathfrak{p}$ in C_S, we see that at least one of the basis elements $y_\mathfrak{q}$ of D_S maps to 0 in C_S. Choose one such $y_\mathfrak{q}$ and let $\mathfrak{q}'$ be the prime of $\mathscr{O}$ lying over the prime $\mathfrak{q}$ of $\mathscr{O}^+$. Since $\mathfrak{q}$ is inert in K/K^+, complex conjugation on K induces a non-trivial automorphism of the residue field $k(\mathfrak{q}')$ that fixes $k(\mathfrak{q})$. We want to show that this $\mathfrak{q}$ divides $F - V$; to do this, it will be enough to show that the image of F in $k(\mathfrak{q}')$ is contained in $k(\mathfrak{q})$, for then the image of $V = \overline{F}$ in $k(\mathfrak{q}')$ will equal that of F, which means that $\mathfrak{q} | (F - V)$.

Let $\mathfrak{p} = \mathfrak{q} \cap R^+$ and let $\mathfrak{p}' = \mathfrak{q}' \cap R$. As we noted just before Proposition 10.5, for $y_\mathfrak{q}$ to map to 0 in C_S, either the degree of $k(\mathfrak{q})$ over $k(\mathfrak{p})$ is even or else $k(\mathfrak{p}') = k(\mathfrak{p})$. In either case, we see that the degree of $k(\mathfrak{q}')$ over $k(\mathfrak{p}')$ is even, which means that $k(\mathfrak{p}')$ is contained in $k(\mathfrak{q})$. Since the image of F in $k(\mathfrak{q}')$ lies inside $k(\mathfrak{p}') = R/\mathfrak{p}'$, the image of F is contained in $k(\mathfrak{q})$, so $\mathfrak{q} | (F - V)$.

On the other hand, suppose there is a $\mathfrak{q}$ of K^+ that divides $F - V$ and that is inert in K/K^+. Let $\mathfrak{q}'$ be the prime of $\mathscr{O}$ lying over $\mathfrak{q}$, let $\mathfrak{p} = \mathfrak{q} \cap R^+$, and let $\mathfrak{p}' = \mathfrak{q}' \cap R$. We see that $k(\mathfrak{p}') \subset k(\mathfrak{q})$, which tells us that the element $y_\mathfrak{q}$ of D maps to 0 in C. Since $y_\mathfrak{q}$ maps to z in $\mathscr{B}(\mathscr{O})$, we have $i^*(z) = 0$ by Proposition 10.4, and i^* is the zero map.

Thus the map i^* is non-zero if and only if K/K^+ is unramified at all finite primes and all the prime ideals of K^+ that divide $F - V$ split in K. Suppose i^* is non-zero; then i^* is injective, so $I_\mathscr{C} = 0$ if and only if $I_{K,\Phi} = 0$. To check the latter condition we evaluate $\chi_{K,\Phi}$ on the totally imaginary element $F - V$ of K and apply Proposition 11.1. Since all the primes of K^+ that divide $F - V$ split in K/K^+, the Artin symbol $((F - V), K/K^+)$ is trivial, so that $\chi_{K,\Phi}(F - V) = \operatorname{sign}(N_\Phi(F - V))$. This shows that $I_\mathscr{C} = 0$ if and only if $N_\Phi(F - V) > 0$. □

(11.4) **Corollary.** *Let $\mathscr{C}$ be an isogeny class of g-dimensional simple ordinary abelian varieties, and let F, V, K, and Φ be as above. If K/K^+ is ramified at some finite prime, or if there is a prime ideal of K^+ that divides $(F - V)$ and that is inert in K/K^+, then there is a principally polarized variety in $\mathscr{C}$. Otherwise, g is even, and there is a principally polarized variety in $\mathscr{C}$ if and only if the Φ-norm of $F - V$ is positive.*

Proof. By the results of §4, it is enough to prove the corresponding statement for the isogeny class of Deligne modules corresponding to $\mathscr{C}$. Now the result follows immediately from Proposition 11.3 and Theorem 5.6. □

Now we can prove Theorem 1.2 from the Introduction.

Proof of Theorem 1.2. Immediate from Corollary 11.4. □

We are left with the problem of calculating the sign of $N_\Phi(F - V)$, at least in certain special cases. The following proposition reduces the task of determining this sign to the task of calculating $N_{K/\mathbf{Q}}(F - V)$, which was accomplished in Proposition 9.5.

(11.5) **Proposition.** *Let q be a power of a prime p, let $\mathscr{C}$ be an isogeny class of simple Deligne modules in $\mathscr{L}_q$ corresponding to a Weil polynomial h of*

degree $2g$, *let* a_g *be the middle coefficient of* h, *and let* K, F, V, v, *and* Φ *be as above. Suppose* K/K^+ *is unramified at all finite primes. Then* $N_\Phi(F-V)$ *satisfies the following conditions, and is determined by them*:

(a) $N_\Phi(F-V)$ *is an integer whose square is* $N_{K/\mathbf{Q}}(F-V)$.
(b) *The integer* $N_\Phi(F-V)$ *is congruent to* a_g *modulo* q.
(c) *If* $q=2$, *then* $N_\Phi(F-V)$ *is congruent to* a_g *modulo* 4.

Proof. We already noted in the proof of Proposition 11.2 that when K/K^+ is unramified at finite primes the Φ-norm $N_\Phi(x)$ of a totally imaginary x in K is a rational number whose square is $N_{K/\mathbf{Q}}(x)$. Applying this to $x=F-V$ shows that $N_\Phi(F-V)$ satisfies condition (a).

We will only sketch a proof of the fact that $N_\Phi(F-V)$ satisfies (b) and (c). Let $F_1, F_2, \ldots, F_g$ be the roots of h in $\mathbf{C}$ that have positive valuation under the p-adic valuation v, and for each $i=1,2,\ldots,g$ let $V_i=q/F_i$, so that the V_i are the remaining roots of h in $\mathbf{C}$ and the V_i have valuation 0. Then the definition of Φ shows that $N_\Phi(F-V)=\prod_{1\le i\le g}(F_i-V_i)$. By comparing this expression to the formula for a_g in terms of the F_i and V_i, one can show that $N_\Phi(F-V)$ satisfies condition (b). A more careful analysis of the formulas for $N_\Phi(F-V)$ and for a_g shows that when $q=2$ condition (c) is satisfied also. The details of these analyses are left to the reader.

Finally we note that condition (a) determines $N_\Phi(F-V)$ up to sign, and since a_g is coprime to q because $\mathscr{C}$ is ordinary, condition (b) (or condition (c), if $q=2$) tells us the sign of $N_\Phi(F-V)$. Thus $N_\Phi(F-V)$ is determined by conditions (a), (b), and (c). □

We will illustrate the use of Corollary 11.4 and Proposition 11.5 in §13.

12. Isogeny classes of two-dimensional ordinary abelian varieties

In this section we will use the results of the previous sections to determine the Weil polynomials of the isogeny classes of two-dimensional ordinary abelian varieties over a finite field that do not contain a principally polarized variety. Our results and methods should be compared with those of [1, §5.4].

Let k be a field with q elements. From Proposition 3.4 we know that the Weil polynomial of a two-dimensional ordinary abelian variety over k is of the form $X^4+aX^3-bX^2+aqX+q^2$, where b is coprime to q. We will prove Theorem 1.3 of the Introduction, which gives necessary and sufficient conditions for such a polynomial to correspond to an isogeny class of abelian varieties not containing a principally polarized variety. We restate Theorem 1.3 here for convenience.

(1.3) **Theorem.** *Let* q *be a power of a prime* p, *let* k *be a field with* q *elements, let* a *and* b *be integers, and let*

$$h=X^4+aX^3-bX^2+aqX+q^2.$$

Then $h=h_{\mathscr{C}}$ *for an isogeny class* $\mathscr{C}$ *of two dimensional ordinary abelian varieties over* k *that does not contain a principally polarized variety if and only if* $q=a^2+b$ *and* b *is a positive integer, coprime to* q, *all of whose prime divisors are* 1 *modulo* 3.

Proof. Suppose $\mathscr{C}$ is an isogeny class of two-dimensional ordinary abelian varieties not containing a principally polarized variety. Then $\mathscr{C}$ must be simple, for

otherwise it would contain a product of two elliptic curves, and elliptic curves are principally polarized. Let $F = F_{\mathscr{C}}$, let $V = V_{\mathscr{C}}$, let $R = R_{\mathscr{C}}$, let $K = K_{\mathscr{C}}$, and let $\mathscr{O} = \mathscr{O}_K$. Let Φ be the CM-type of K obtained from the embedding $\varepsilon: W \hookrightarrow \mathbf{C}$ we chose in §5. Since $\mathscr{C}$ is simple we can apply Corollary 11.4, and we see that K/K^+ is unramified at all finite primes, that no primes of $\mathscr{O}^+$ that are inert in K/K^+ divide $(F - V)$, and that $N_\Phi(F - V) < 0$.

(12.1) **Lemma.** *Let notation and assumptions be as above. The field K is a Galois extension of $\mathbf{Q}$, with Galois group $G \cong V_4$.*

Proof. Let π and π' be the two roots of $h_{\mathscr{C}}$ in $\mathbf{C}$ that have positive imaginary parts. Then the four roots of $h_{\mathscr{C}}$ in $\mathbf{C}$ are π, $\overline{\pi} = q/\pi$, π', and $\overline{\pi}' = q/\overline{\pi}$. Let $N = \mathbf{Q}(\pi, \pi')$.

Suppose π and $\overline{\pi}'$ are not coprime in $\mathscr{O}_N$. Then there is a p-adic valuation v of $\overline{\mathbf{Q}} \subset \mathbf{C}$ such that $v(\pi) > 0$ and $v(\overline{\pi}') > 0$. Let Ψ be the CM-type of N corresponding to v; we have $N_\Psi(F-V) > 0$. But the proof of Proposition 11.2 shows that $N_\Psi(F-V)$ and $N_\Phi(F-V)$ have the same sign, and we already know that $N_\Phi(F - V) < 0$. This contradiction shows that π and $\overline{\pi}'$ are coprime in $\mathscr{O}_N$.

Since $\pi | q = \pi'\overline{\pi}'$ and since π and $\overline{\pi}'$ are coprime, we have $\pi | \pi'$, and since π and π' have the same norm, the ideals (π) and (π') of $\mathscr{O}_N$ are equal. Let H be the subgroup of $\mathrm{Gal}(N/\mathbf{Q})$ defined by $H = \{\sigma \mid (\sigma\pi) = (\pi)\}$. Then H properly contains $\mathrm{Gal}(N/\mathbf{Q}(\pi))$ but H does not contain complex conjugation, so $\mathbf{Q}(\pi)$ contains a quadratic subfield that is different from $\mathbf{Q}(\pi)^+$. This shows that $\mathbf{Q}(\pi)$ is a Galois extension of $\mathbf{Q}$ with group V_4, and since $K \cong \mathbf{Q}(\pi)$ we are done. □

Let ρ be the non-identity element of the Galois group G of $K/\mathbf{Q}$ that fixes K^+. Let σ be the non-identity element of the subgroup H of G defined in the proof of Lemma 12.1, so that $(F) = (\sigma F)$, and let L be the fixed field of $\{1, \sigma\}$. Finally, let M be the fixed field of $\{1, \sigma\rho\}$, so that K^+, L, and M are the three quadratic subfields of K, and L and M are imaginary.

Let $\Delta_L \in \mathbf{Z}$ and $\Delta_M \in \mathbf{Z}$ be the discriminants of the fields L and M, respectively. We have $L = \mathbf{Q}(\sqrt{\Delta_L})$ and $M = \mathbf{Q}(\sqrt{\Delta_M})$. Since K/K^+ is unramified at finite primes, we have $(\Delta_L, \Delta_M) = 1$.

Since $\mathscr{C}$ contains no principally polarized variety we must have $I_{K,\Phi} \neq 0$, so by Proposition 11.1 we have $X_{K,\Phi} = -1$, which means that $\chi_{K,\Phi}(x) = -1$ for every totally imaginary x in K. Take for x the totally imaginary element $\sqrt{\Delta_M}$. Now, if φ is one of the elements of our CM-type Φ, then the other element must be $\varphi\sigma$, since $(\sigma F) = (F)$. Since $\sigma(\sqrt{\Delta_M}) = -\sqrt{\Delta_M}$, we find that $N_\Phi(\sqrt{\Delta_M}) = -\Delta_M > 0$. Since $\chi_{K,\Phi}(\sqrt{\Delta_M}) = -1$, the Artin symbol $((\sqrt{\Delta_M}), K/K^+)$ must be -1. Taking norms from K^+ to $\mathbf{Q}$, we find that $((\Delta_M), L/\mathbf{Q}) = -1$. In particular, $\Delta_M \neq -4$, so $M \neq \mathbf{Q}(i)$.

Similarly we find that $N_\Phi(\sqrt{\Delta_L}) = \Delta_L < 0$, so that $((\Delta_L), M/\mathbf{Q}) = 1$.

(12.2) **Lemma.** *Let notation and assumptions be as above. Then $\Delta_M = -3$, and there is a primitive cube root of unity $\zeta \in M$ and an integer α of L such that $F = \zeta\alpha$.*

Proof. Let $\xi = \sigma(F)/F$. Then (ξ) is the unit ideal of $\mathscr{O}$ and $\varphi(\xi)$ has magnitude 1 for every embedding φ of K into $\mathbf{C}$, so ξ is a root of unity. Now there are three possibilities: The first possibility is that ξ is an element of L. The second is that ξ is an element of M but not of L. This implies that M is a cyclotomic field of degree 2 that is not $\mathbf{Q}(i)$; that is, M must be $\mathbf{Q}(\zeta_3)$. The third possibility is that ξ lies neither in L nor in M. In this case, K must be a cyclotomic field with Galois group V_4 that is unramified over its maximal real subfield at all finite primes; that is, K must be $\mathbf{Q}(\zeta_{12})$, and we find that $M = \mathbf{Q}(\zeta_3)$ and $L = \mathbf{Q}(i)$. In all three cases, we can find a root of unity $\zeta \in M$ such that $\omega = \xi\zeta^2$ is an element of L. Let $\alpha = F/\zeta$. Then $\sigma(\alpha) = \omega\alpha$, and since $\omega \in L$, we have $\alpha = \sigma^2(\alpha) = \omega^2\alpha$, so $\omega = \pm 1$.

Suppose, to get a contradiction, that $\omega = -1$. The different $\mathfrak{d}_{K/L}$ is generated as an $\mathscr{O}_K$-ideal by the set of elements of the form $\sigma\beta - \beta$, for $\beta \in \mathscr{O}_K$. Therefore $\mathfrak{d}_{K/L}$ contains 2α and $2\overline{\alpha}$ and hence also $2F$ and $2V$. Since F and V are coprime by Lemma 4.12, the different $\mathfrak{d}_{K/L}$ also contains 2, so $\mathfrak{d}_{K/L} | 2\mathscr{O}_K$. This implies that the different of $M/\mathbf{Q}$ divides 2, so that the discriminant Δ_M divides 4. But then we must have $\Delta_M = -4$, which is not the case, as we noted above.

Thus $\omega = 1$ and $\sigma(\alpha) = \alpha$; that is, $\alpha \in L$. Since $F = \zeta\alpha$ is not in L, it must be that $\zeta \notin L$. As above, this shows that $\Delta_M = -3$, so that ζ is a root of unity, different from ± 1, in $\mathbf{Q}(\zeta_3)$. Replacing α by $-\alpha$ and ζ by $-\zeta$, if necessary, we see that $F = \zeta\alpha$ is of the form claimed in the statement of the lemma. □

Now that we know that $M = \mathbf{Q}(\zeta)$, the fact that $((\Delta_L), M/\mathbf{Q}) = 1$ implies that $|\Delta_L| \equiv 1 \bmod 3$, so that $\Delta_L \equiv -1 \bmod 3$.

The next lemma will help us make use of the knowledge that all of the primes of K^+ that divide $(F - V)$ split in K/K^+.

(12.3) **Lemma.** *Let notation and assumptions be as above and let* $\mathfrak{p}$ *be a prime of* K^+ *lying over a prime* ℓ *of* $\mathbf{Q}$.

(a) *Suppose that* $\ell \nmid \Delta_L\Delta_M$. *Then* $\mathfrak{p}$ *splits in* K/K^+ *if and only if* ℓ *splits in* $M/\mathbf{Q}$ *or in* $L/\mathbf{Q}$.

(b) *Suppose that* $\ell | \Delta_L$. *Then* $\mathfrak{p}$ *splits in* K/K^+ *if and only if* ℓ *splits in* $M/\mathbf{Q}$.

(c) *Suppose that* $\ell | \Delta_M = -3$. *Then* $\mathfrak{p}$ *does not split in* K/K^+.

Proof. Suppose $\ell \nmid \Delta_L\Delta_M$, so that ℓ does not ramify in $K/\mathbf{Q}$. Then $\mathfrak{p}$ is inert in K/K^+ if and only if the decomposition group $D_{\mathfrak{p}}$ of $\mathfrak{p}$ is $\{1, \rho\}$, which is the case if and only if ℓ is inert in both $L/\mathbf{Q}$ and $M/\mathbf{Q}$. The contrapositive of this statement is statement (a) of the lemma. Now suppose $\ell | \Delta_L$. Then ℓ ramifies in $K/\mathbf{Q}$, so that $\mathfrak{p}$ splits in K/K^+ if and only if there are two primes of K over ℓ, which in turn holds if and only if ℓ splits in $M/\mathbf{Q}$. This is statement (b). Finally, suppose $\ell = 3$. Then ℓ ramifies in $M/\mathbf{Q}$ and ℓ is inert in $L/\mathbf{Q}$, because $\Delta_L \equiv -1 \bmod 3$. Thus $\mathfrak{p}$ must be inert in K/K^+. □

Let b be the positive integer $-N_\Phi(F - V)$.

(12.4) **Lemma.** *Let notation and assumptions be as above. Then every prime dividing* b *is* 1 *modulo* 3.

Proof. Since the primes of $\mathbf{Q}$ that split in $M/\mathbf{Q}$ are the primes that are 1 modulo 3, it will be enough to show that every prime dividing b splits in $M/\mathbf{Q}$. So suppose ℓ is a prime divisor of b. Then there is a prime $\mathfrak{p}$ of K^+ lying over ℓ that divides the ideal $(F - V)$. Our assumptions on the isogeny class $\mathscr{C}$ imply that $\mathfrak{p}$ splits in K/K^+; by Lemma 12.3, this shows that $\ell \neq 3$ and that either ℓ splits in $M/\mathbf{Q}$ or ℓ splits in $L/\mathbf{Q}$. If ℓ splits in $M/\mathbf{Q}$ we are done, so assume that ℓ splits in $L/\mathbf{Q}$.

An easy calculation shows that $N_\Phi(F - V) = \alpha^2 + \alpha\overline{\alpha} + \overline{\alpha}^2$, where for convenience we denote $\rho(\alpha)$ by $\overline{\alpha}$. Since ℓ splits in $L/\mathbf{Q}$, there is a ring homomorphism $s: \mathscr{O}_L \to \mathbf{Z}/\ell\mathbf{Z}$. Since ℓ divides b we have $s(\alpha)^2 + s(\alpha)s(\overline{\alpha}) + s(\overline{\alpha})^2 = 0$, and since $(F, V) = (\alpha, \overline{\alpha}) = 1$, neither α nor $\overline{\alpha}$ maps to 0 via s. Thus, $\beta = s(\alpha)/s(\overline{\alpha})$ is a root in $\mathbf{Z}/\ell\mathbf{Z}$ of the polynomial $X^2 + X + 1$. Since $\ell \neq 3$, this shows that ℓ splits in M, the splitting field of $X^2 + X + 1$ over $\mathbf{Q}$. □

Let a be the rational integer $\mathrm{Tr}_{L/\mathbf{Q}}(\alpha) = \alpha + \overline{\alpha}$. From the equality $FV = q$ we see that $\alpha\overline{\alpha} = q$, and it is easy to check that this equality and the fact that $b = -(\alpha^2 + \alpha\overline{\alpha} + \overline{\alpha}^2)$ imply that $q = a^2 + b$. It is also easy to check that the minimal polynomial of $F = \zeta\alpha$ is $X^4 + aX^3 - bX^2 + aqX + q^2$, and since $\mathscr{C}$ is ordinary, the middle coefficient $-b$ is coprime to q. This completes the proof of the "only if" part of Theorem 1.3.

Now we turn to the "if" part of the theorem. Suppose $h = X^4 + aX^3 - bX^2 + aqX + q^2$, where $q = a^2 + b$ and where a and b are integers such that b is positive and coprime to q, and such that all of the prime divisors of b are 1 modulo 3. Let ζ be a primitive cube root of unity in $\mathbf{C}$, and let α be a root in $\mathbf{C}$ of the polynomial $f = X^2 - aX + q$. Let $L = \mathbf{Q}(\alpha)$ and $M = \mathbf{Q}(\zeta)$. The discriminant Δ of f is equal to $a^2 - 4q$; from the equality $\Delta = -b - 3q$ we see that Δ is negative and is congruent to 2 modulo 3, so L is an imaginary quadratic field that is different from M. Let $K = \mathbf{Q}(\alpha, \zeta)$ and let $F = \zeta\alpha$. It is easy to check that F is a Weil q-number with minimal polynomial h. Let $\mathscr{C}$ be the isogeny class of simple ordinary abelian varieties corresponding to h.

Let K^+ be the maximal real subfield of the CM-field K. Since Δ is coprime to 3, the field extension K/K^+ is unramified at all finite primes. One can check that the Φ-norm of $F - q/F$ is equal to $-b$. Since all the primes dividing b split in $M/\mathbf{Q}$, all the primes of K^+ dividing $(F - q/F)$ split in K/K^+. Thus, by Corollary 11.4, the isogeny class $\mathscr{C}$ does not contain a principally polarized variety. This completes the proof of Theorem 1.3. □

(12.5) **Corollary.** *Let q be a power of a prime number p and let k be a field with q elements. There is a bijection between the set of isogeny classes of two-dimensional ordinary abelian varieties over k that do not contain principally polarized varieties and the set of pairs of integers (a, b) such that $q = a^2 + b$ and b is a positive integer, coprime to q, all of whose prime divisors are 1 modulo 3.*

Proof. Immediate from Theorem 1.3. □

(12.6) **Corollary.** *Suppose A is a two-dimensional ordinary abelian variety over a finite field k that is not isogenous to a principally polarized variety. Then over the cubic extension of k the variety A becomes isogenous to a product of an elliptic curve with itself.*

Proof. We saw in the proof of Theorem 1.3 that the Weil number of the isogeny class of such an A is of the form $\pi = \zeta\alpha$, where α is quadratic over $\mathbf{Q}$ and ζ is a cube root of unity. The Weil polynomial of this isogeny class over the cubic extension of k is the characteristic polynomial of $\pi^3 = \alpha^3$, which is the square of the minimal polynomial of α^3. This factorization of the Weil polynomial corresponds to the factorization of the isogeny class of A over the cubic extension of the base field into the product of an isogeny class of elliptic curves with itself. □

(12.7) **Corollary.** *Suppose that q is a power of 3 or that $q = r^2$ for a prime power r that is 2 modulo 3. Let k be a field with q elements. Then every isogeny class of two-dimensional ordinary abelian varieties over k contains a principally polarized variety.*

Proof. If q is a power of 3 then it is not possible to write q as $a^2 + b$ where b is 1 modulo 3; to see this, simply look at $a^2 + b$ modulo 3. Thus, by Theorem 1.3 every isogeny class of two-dimensional ordinary abelian varieties over k contains a principally polarized variety.

Suppose $q = r^2$ for some r that is 2 modulo 3. Let a be any integer such that $q - a^2$ is positive. Then $r - a$ and $r + a$ are both positive divisors of $q - a^2$, and at least one of these numbers is not 1 modulo 3. Hence $q - a^2$ has prime divisors that are not 1 modulo 3. Again by Theorem 1.3, every isogeny class of two-dimensional ordinary abelian varieties over k contains a principally polarized variety. □

13. Applications and examples

We saw in Theorem 1.3 that most isogeny classes of simple two-dimensional ordinary abelian varieties over a finite field k contain a principally polarized variety. By combining this information with a theorem of Weil, as interpreted by Oort and Ueno, we obtain the following theorem, which can be viewed as an extension of [16, Theorem 1.2, p. 32].

(13.1) **Definition** (see [14]). A *good curve* over a field k is a reduced but possibly reducible curve C over k that is stable (in the sense of [4, Definition 1.1]) and whose Jacobian $\mathrm{Pic}^0(C)$ is an abelian variety. Equivalently, a good curve over k is a curve C over k such that the curve $C_{\overline{k}}$ over the algebraic closure $\overline{k}$ of k satisfies the following conditions:

(a) The curve $C_{\overline{k}}$ is connected and reduced.
(b) If $C_{\overline{k}}$ has more than one component, then every component of genus zero intersects at least three other components.
(c) Every singularity of $C_{\overline{k}}$ is a node.
(d) Every component of $C_{\overline{k}}$ is a non-singular curve.
(e) The dual graph of $C_{\overline{k}}$ is a tree; here the dual graph is the graph constructed by taking one vertex v_D for every component D and by drawing one edge between v_D and $v_{D'}$ for every point of intersection between D and D'.

The *genus* of a good curve is the sum of the genera of its components.

(13.2) *Remark.* The characterization of good curves in [14] is incorrect.

(13.3) **Theorem.** *Let k be a field with q elements and let $\mathscr{C}$ be an isogeny class of two-dimensional ordinary abelian varieties over k. Let*

$$h = X^4 + aX^3 - bX^2 + aqX + q^2$$

be the Weil polynomial for $\mathscr{C}$, so that b is coprime to q. Then $\mathscr{C}$ contains the generalized Jacobian of a good curve C over k of genus two if and only if either $q \neq a^2 + b$ or $b < 0$ or b has a prime divisor that is not 1 modulo 3.

Proof. Suppose that either $q \neq a^2 + b$ or $b < 0$ or b has a prime divisor that is not 1 modulo 3. Then from Theorem 1.3 we know that $\mathscr{C}$ contains a principally polarized variety A. Let λ be a principal polarization of A. Then there is a good curve C over $\overline{k}$ of genus two whose canonically polarized generalized Jacobian is isomorphic to $(A_{\overline{k}}, \lambda_{\overline{k}})$; this is a result of Weil ([21, Satz 2, p. 37]) as restated by Oort and Ueno ([14, Theorem 4, p. 378]).

Let σ be the qth-powering automorphism of $\overline{k}/k$. Since A and λ are defined over k, there is an isomorphism $\psi: (A_{\overline{k}}, \lambda_{\overline{k}})^{\sigma} \cong (A_{\overline{k}}, \lambda_{\overline{k}})$. Because C is either a hyperelliptic curve or two elliptic curves joined together at a point, Torelli's theorem says that there is an isomorphism $\varphi: C \to C^{\sigma}$ that gives rise to the isomorphism ψ. Since the Galois group G of $\overline{k}/k$ is freely generated as a profinite group by σ, the isomorphism φ gives us an action of G on C. By Weil descent, this action of G defines a curve D over k such that $D_{\overline{k}}$ with its natural G-action is isomorphic to C with the G-action we just defined. Let (B, μ) be the canonically polarized Jacobian of D; then Torelli's theorem shows that there is a G-equivariant isomorphism from $(B_{\overline{k}}, \mu_{\overline{k}})$ to $(A_{\overline{k}}, \lambda_{\overline{k}})$. Thus $(B, \mu) \cong (A, \lambda)$, and A is isomorphic to the Jacobian of D.

On the other hand, if $q = a^2 + b$ and b is a positive number all of whose prime factors are 1 modulo 3, then by Theorem 1.3 there is no principally polarized variety in $\mathscr{C}$, so in particular there is no Jacobian in $\mathscr{C}$. □

We saw in Corollary 12.6 that if A is a two-dimensional ordinary abelian variety over a finite field k and if A is not isogenous to a principally polarized variety, then over the cubic extension ℓ of k the variety $A \times_k \ell$ is isogenous to a product of an elliptic curve with itself; in particular, this means that A is not absolutely simple. The obvious question is whether there exists an absolutely simple abelian variety over a finite field k that is not isogenous to a principally polarized variety. The following examples show that such varieties do exist.

(13.4) **Example.** Let $\zeta = \zeta_{20}$ be a primitive 20th root of unity and let $K = \mathbf{Q}(\zeta)$. Since 4 and 5 both divide 20, the field K is unramified over its maximal real subfield K^+ except at the infinite primes. The prime $p = 41$ of $\mathbf{Q}$ splits completely in K, and one of the primes of K lying over it is the principal ideal generated by $\alpha = 1 + \zeta - \zeta^5$; one can verify this by noting that $N_{K/\mathbf{Q}}(\alpha) = p$. Let $\pi = \zeta^2 \cdot \alpha^{(1)+(3)+(7)+(11)}$, where the exponents in parentheses are viewed as elements of the Galois group $G \cong (\mathbf{Z}/20\mathbf{Z})^*$ of K over $\mathbf{Q}$. The subset $\{(1 \bmod 20), (3 \bmod 20), (7 \bmod 20), (11 \bmod 20)\}$ of G is fixed by no non-trivial subgroup of G, so the ideal (π) is not the lift of an ideal from a proper subfield of K. In particular, π is not contained in any proper subfield of K.

Complex conjugation on K corresponds to the element $(-1 \bmod 20)$ of G, so $\pi\overline{\pi} = N_{K/\mathbf{Q}}(\alpha) = p$. Thus π is a Weil number. The minimal polynomial of

π is

$$h = X^8 - 2X^7 - 87X^6 + 106X^5 + 4205X^4 + 4346X^3 - 146247X^2 - 137842X + 2825761,$$

and since p does not divide 4205, the polynomial h is an ordinary Weil polynomial. We can calculate, using Proposition 9.5 for example, that the norm of $\pi - \overline{\pi}$ is $93025 = 5^2 \cdot 61^2$. The decomposition group of 5 in $K/\mathbf{Q}$ is the subgroup of G generated by $(13 \bmod 20)$. Since this subgroup does not contain $(-1 \bmod 20)$, every prime of K^+ lying over 5 splits in K. The decomposition group of 61 in $K/\mathbf{Q}$ is the subgroup of G generated by $(61 \bmod 20) = (1 \bmod 20)$, so 61 splits completely in K. In particular, we see that every prime of K^+ dividing the ideal $(\pi - \overline{\pi})$ splits in K.

Finally, we notice that the middle coefficient 4205 of h is congruent to $-5 \cdot 61$ modulo p, so that Proposition 11.5 tells us that the Φ-norm of $\pi - \overline{\pi}$ is negative. By Corollary 11.4, the isogeny class $\mathscr{C}$ of ordinary abelian varieties corresponding to h does not contain a principally polarized variety.

Let ℓ be a field extension of k of degree n. The isogeny class $\mathscr{C}_\ell$ of ordinary abelian varieties over ℓ that contains the lifts to ℓ of the varieties in $\mathscr{C}$ corresponds to the Weil number π^n. The same argument that showed that π is not contained in a proper subfield of K shows that π^n does not lie in a proper subfield of K. This means that the characteristic polynomial of π^n is irreducible, so that $\mathscr{C}_\ell$ is a simple isogeny class. Thus $\mathscr{C}$ is an absolutely simple isogeny class of four-dimensional ordinary abelian varieties over $\mathbf{F}_{41}$ that does not contain a principally polarized variety.

(13.5) **Example.** Let $\zeta = \zeta_{24}$ be a primitive 24th root of unity, and let $K = \mathbf{Q}(\zeta)$. Again we find that K/K^+ is unramified at all finite primes. The prime $p = 73$ of $\mathbf{Q}$ splits completely in K, and one of the primes of K lying over it is generated by $\alpha = \zeta^8 + \zeta^3 - 1$. Let $\pi = \zeta^6 \cdot \alpha^{(1)+(5)+(7)+(13)}$, where again the exponents in parentheses are viewed as elements of $\mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/24\mathbf{Z})^*$. Then $\pi\overline{\pi} = 73$, and the minimal polynomial of π is

$$h = X^8 - 16X^7 + 64X^6 + 776X^5 - 13289X^4 + 56648X^3 + 341056X^2 - 6224272X + 28398241;$$

since p does not divide 13289, the polynomial h is an ordinary Weil polynomial. One can check that $N_{K/\mathbf{Q}}(\pi - \overline{\pi}) = 194481 = 3^4 \cdot 7^4$, that every prime of K^+ lying over 3 or 7 splits in K/K^+, and that the middle coefficient of h is congruent to $-3^2 \cdot 7^2$ modulo p. Then Corollary 11.4 and Proposition 11.5 tell us that the isogeny class $\mathscr{C}$ of ordinary abelian varieties over $\mathbf{F}_{73}$ corresponding to h does not contain a principally polarized variety. As in the previous example, $\mathscr{C}$ consists of absolutely simple varieties.

In each of the two previous examples we found an isogeny class $\mathscr{C}$ of abelian varieties over a finite field k that does not contain a principally polarized variety. However, for each of these examples there is another isogeny class $\mathscr{D}$ of abelian varieties over k that does contain a principally polarized variety and such that the isogeny classes $\mathscr{C}_{\overline{k}}$ and $\mathscr{D}_{\overline{k}}$ over the algebraic closure $\overline{k}$ of k are equal. The following example shows that it is possible to find an isogeny class $\mathscr{C}$ such that no such $\mathscr{D}$ exists.

(13.6) **Example.** Let $K = \mathbf{Q}(\sqrt{-2}, \sqrt{-7}, \sqrt{-11})$, let $u = \sqrt{-2}$, let $v = (1+\sqrt{-7})/2$, let $w = (1+\sqrt{-11})/2$, and let σ (respectively, τ, ρ) be the non-trivial automorphism of K that fixes v and w (respectively, u and w, u and v). The discriminants of $\mathbf{Q}(u)$ and $\mathbf{Q}(v)$ and $\mathbf{Q}(w)$ are coprime, so the field K is unramified over $K^+ = \mathbf{Q}(\sqrt{14}, \sqrt{22})$ at all finite primes. Let $p = 617$; the prime p splits completely in $K/\mathbf{Q}$, and one of the primes lying over it is generated by $\alpha = u+v+w$. Let $\pi = \alpha^{1+\sigma+\tau+\rho}$. Complex conjugation is given by the automorphism $\sigma\tau\rho$, so $\pi \cdot \overline{\pi} = N_{K/\mathbf{Q}}(\alpha) = p$ and π is a Weil number. The minimal polynomial of π is

$$h = X^8 - 112X^7 + 5404X^6 - 156688X^5 + 3788262X^4 \\ - 96676496X^3 + 2057243356X^2 - 26307132656X + 144924114721,$$

which is an ordinary Weil polynomial. The norm of $\pi - \overline{\pi}$ is $2^{16} \cdot 3^4 \cdot 67^2$. One can check that the decomposition group of 2 in $K/\mathbf{Q}$ is $\{1, \sigma, \rho, \sigma\rho\}$, that the decomposition group of 3 is $\{1, \tau\}$, and that the decomposition group of 67 is $\{1\}$. Since none of these groups contains $\sigma\tau\rho$, every prime of K^+ dividing $(\pi - \overline{\pi})$ splits in K/K^+. Finally, one notes that the middle coefficient of h is congruent to $-2^8 \cdot 3^2 \cdot 67$ modulo 617, so the isogeny class $\mathscr{C}$ of ordinary abelian varieties over $k = \mathbf{F}_{617}$ corresponding to h contains no principally polarized varieties. Also, $\mathscr{C}$ is absolutely simple, because the ideal (π) is fixed by no non-trivial subgroup of the Galois group of $K/\mathbf{Q}$.

Suppose $\pi' \in K'$ is a Weil number corresponding to an isogeny class $\mathscr{D}$ of ordinary abelian varieties over k that becomes equal to $\mathscr{C}$ over $\overline{k}$. Then the same statement is true over some finite extension ℓ of k, say of degree n. Then we must have $\mathbf{Q}(\pi^n) \cong \mathbf{Q}(\pi'^n)$, with the isomorphism taking π^n to π'^n. Since $\mathscr{C}$ is absolutely simple we have $K = \mathbf{Q}(\pi^n)$, so we have $K = \mathbf{Q}(\pi^n) \cong \mathbf{Q}(\pi'^n) \subset K'$. Since K' and K both have degree four over $\mathbf{Q}$, we can take $K' = K$ and we can think of π' as an element of K. Consider the element $\varepsilon = \pi/\pi'$ of K. The element ε is a unit of the ring of integers of K because π and π' generate the same ideal of K, since they have equal nth powers. Also, since $\varphi(\pi)$ and $\varphi(\pi')$ have absolute value $p^{1/2}$ for every embedding φ of K into $\mathbf{C}$, the unit ε must have absolute value 1 under every such embedding. Thus ε is a root of unity. Now, the only roots of unity in K are 1 and -1, so either $\pi' = \pi$ or $\pi' = -\pi$. In either case, one can check from the minimal polynomial of π' that the isogeny class $\mathscr{D}$ also contains no principally polarized varieties.

Let k be a finite field with q elements. Suppose $\mathscr{D}$ is an isogeny class of two-dimensional ordinary abelian varieties over k, and suppose $\mathscr{E}$ is an isogeny class of ordinary elliptic curves over k. Let $\mathscr{C} = \mathscr{D} \times \mathscr{E}$. We will investigate circumstances under which the obstruction element $I_{\mathscr{C}}$ is non-zero.

(13.7) **Example.** Suppose the isogeny class $\mathscr{D}$ corresponds to a Weil polynomial

$$h = X^4 + aX^3 - bX^2 + aqX + q^2$$

and let $g = X^2 - tX + q$ be the Weil polynomial for $\mathscr{E}$. Since $R_{\mathscr{C}} = R^+_{\mathscr{C}}[T]/(T^2 - (F+V)T + q)$, the natural injection $R_{\mathscr{C}} \hookrightarrow R_{\mathscr{D}} \times R_{\mathscr{E}}$ is an

isomorphism if and only if $R_{\mathscr{C}}^+ \hookrightarrow R_{\mathscr{D}}^+ \times R_{\mathscr{E}}^+$ is an isomorphism. This last injection is an isomorphism if and only if the resultant of h^+ and g^+ is ± 1, where h^+ and g^+ are the minimal polynomials of $F_{\mathscr{D}}+V_{\mathscr{D}}$ and $F_{\mathscr{E}}+V_{\mathscr{E}}$, respectively. When $R_{\mathscr{C}} \hookrightarrow R_{\mathscr{D}} \times R_{\mathscr{E}}$ is an isomorphism, we have $\mathscr{B}(\mathscr{C}) = \mathscr{B}(\mathscr{D}) \oplus \mathscr{B}(\mathscr{E})$ and $I_{\mathscr{C}} = (I_{\mathscr{D}}, I_{\mathscr{E}})$. Since $\mathscr{B}(\mathscr{E}) = 0$ by Example 10.7, we see that in this case $I_{\mathscr{C}} = 0$ if and only if $I_{\mathscr{D}} = 0$.

One can show, using Remark 9.3 for example, that $h^+ = X^2 + aX - (b + 2q)$ and that $g^+ = X - t$, so the resultant of g^+ and h^+ is $t^2 + at - (b + 2q)$. Suppose, for example, we take $p = q = 17$, $a = 2$, $b = 13$, and $t = 6$. Then Theorem 1.3 tells us that h is a Weil polynomial and that $I_{\mathscr{D}} \neq 0$. The resultant of g^+ and h^+ is 1, so $I_{\mathscr{C}} \neq 0$.

(13.8) **Example.** Let $p = q = 17$ and let $h = X^4 + 2X^3 - 13X^2 + 34X + 289$ be as in the previous example, so that h corresponds to an isogeny class $\mathscr{D}$ of two-dimensional ordinary abelian varieties with $I_{\mathscr{D}} \neq 0$. We will find an isogeny class $\mathscr{E}'$ of elliptic curves over $\mathbf{F}_p$ such that $I_{\mathscr{D}\times\mathscr{E}'} = 0$.

Let $K = K_{\mathscr{D}}$ and let $\mathscr{O} = \mathscr{O}_K$. The methods used in the proof of Theorem 1.3 show that $K = \mathbf{Q}(\sqrt{-3}, \sqrt{-1})$, so that $K^+ = \mathbf{Q}(\sqrt{3})$. The prime 2 ramifies in $\mathscr{O}^+$, say $2\mathscr{O}^+ = \mathfrak{t}^2$ for some ideal $\mathfrak{t}$ of $\mathscr{O}^+$. The prime $\mathfrak{t}$ remains inert in $\mathscr{O}$, so the image of $\mathscr{O}^+/\mathfrak{t}$ in $\mathscr{B}(\mathscr{O})$ is non-zero, and its image in $\mathscr{B}(R_{\mathscr{D}})$ is $I_{\mathscr{D}}$. Let $\mathfrak{p} = R_{\mathscr{D}}^+ \cap \mathfrak{t}$. The prime $\mathfrak{p}$ has residue field $\mathbf{F}_2$ (because $\mathfrak{t}$ does), and since h factors modulo 2 as $(X^2 + X + 1)^2$, the prime $\mathfrak{p}$ is inert in $R_{\mathscr{D}}/R_{\mathscr{D}}^+$.

Let $g = X^2 - X + 17$. There is an isogeny class $\mathscr{E}'$ of ordinary elliptic curves with $g = h_{\mathscr{E}'}$. Since g is irreducible modulo 2, the prime $\mathfrak{q} = (2)$ of $R_{\mathscr{E}'}^+ = \mathbf{Z}$ is inert in $R_{\mathscr{E}'}$.

Let $\mathscr{C}$ be the isogeny class of three-dimensional ordinary abelian varieties over $\mathbf{F}_p$ corresponding to the Weil polynomial hg. Because hg factors modulo 2 as $(X^2 + X + 1)^3$, the ring $R_{\mathscr{C}}$ has exactly one prime $\mathfrak{r}'$ lying over 2, corresponding to the homomorphism $R_{\mathscr{C}} \to \mathbf{F}_4$ that sends $F_{\mathscr{C}}$ to $\alpha \in \mathbf{F}_4$, where $\alpha^2 + \alpha + 1 = 0$. The image of $R_{\mathscr{C}}^+ = \mathbf{Z}[F_{\mathscr{C}} + V_{\mathscr{C}}]$ under reduction modulo $\mathfrak{r}'$ is equal to $\mathbf{F}_2$, because $F_{\mathscr{C}} + V_{\mathscr{C}}$ lands on the trace of α, which is 1. Thus, $R_{\mathscr{C}}^+$ has one prime $\mathfrak{r}$ over 2, and $\mathfrak{r}$ is inert in $R_{\mathscr{C}}/R_{\mathscr{C}}^+$. The prime $\mathfrak{r}$ is singular, since it contains the two minimal ideals of $R_{\mathscr{C}}^+$ that lie under $R_{\mathscr{D}}^+ \times 0$ and $0 \times R_{\mathscr{E}'}^+$.

Now apply Proposition 10.5 with $R = R_{\mathscr{C}}$ and $S = R_{\mathscr{D}} \times R_{\mathscr{E}'}$. The primes $\mathfrak{p}' = \mathfrak{p} \times R_{\mathscr{E}'}^+$ and $\mathfrak{q}' = R_{\mathscr{D}}^+ \times \mathfrak{q}$ of S^+ both lie over $\mathfrak{r}$, so in the notation of Proposition 10.5, both $y_{\mathfrak{p}'}$ and $y_{\mathfrak{q}'}$ map to the element $x_{\mathfrak{r}}$ of C_S. Thus $y_{\mathfrak{p}'}$ and $y_{\mathfrak{q}'}$ have the same image in $\mathscr{B}(R)$, so the elements $(I_{\mathscr{D}}, 0)$ and $(0, I_{\mathscr{E}'})$ of $\mathscr{B}(S)$ have the same image in $\mathscr{B}(R)$. Now $I_{\mathscr{E}'} = 0$ by Example 10.7, so both $I_{\mathscr{D}}$ and $I_{\mathscr{E}'}$ map to 0 in $\mathscr{B}(R)$. By definition $I_{\mathscr{C}}$ is the sum of the images of $I_{\mathscr{D}}$ and $I_{\mathscr{E}'}$ in $\mathscr{B}(R)$, so $I_{\mathscr{C}} = 0$. This shows that $\mathscr{C}$ contains a principally polarized variety, even though $\mathscr{D}$ does not.

To summarize: In the previous two examples we have found isogeny classes $\mathscr{E}$ and $\mathscr{E}'$ of elliptic curves and an isogeny class $\mathscr{D}$ of two-dimensional varieties with $I_{\mathscr{E}} = I_{\mathscr{E}'} = 0$ and with $I_{\mathscr{D}} \neq 0$, and such that $I_{\mathscr{D}\times\mathscr{E}} \neq 0$ and $I_{\mathscr{D}\times\mathscr{E}'} = 0$. These examples show that the obstruction element of an isogeny class really does depend not just on the obstruction elements of its factors but also on how the factors interact with one another.

REFERENCES

1. L. M. Adleman and M.-D. A. Huang, *Primality testing and abelian varieties over finite fields*, Lecture Notes in Math., vol. 1512, Springer-Verlag, New York, 1992.
2. J. V. Armitage, *On a theorem of Hecke in number fields and function fields*, Invent. Math. **2** (1967), 238–246.
3. P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.
4. P. Deligne and D. Mumford, *The irreducibility of the space of curves of a given genus*, Inst. Hautes Études Sci. Publ. Math. No. 36 (1969), 75–109.
5. A. Fröhlich, *Local fields*, Algebraic Number Theory (J. W. S. Cassels and A. Fröhlich, eds.), Academic Press, New York, 1986, pp. 1–41.
6. T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.
7. E. W. Howe, *Kernels of polarizations of abelian varieties over finite fields*, submitted for publication.
8. N. Katz, *Serre-Tate local moduli*, Surfaces Algébriques (J. Giraud, L. Illusie, and M. Raynaud, eds.), Lecture Notes in Math., vol. 868, Springer-Verlag, Berlin, 1981, pp. 138–202.
9. M.-A. Knus, *Quadratic and Hermitian forms over rings*, Grundlehren Math. Wiss., vol. 294, Springer-Verlag, New York, 1991.
10. W. Messing, *The crystals associated to Barsotti-Tate groups*, Lecture Notes in Math., vol. 264, Springer-Verlag, Berlin, 1972.
11. J. S. Milne, *Abelian varieties*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, New York, 1986, pp. 103–150.
12. D. Mumford, *Abelian varieties*, Oxford University Press, Oxford, 1985.
13. M. V. Nori and V. Srinivas, *Canonical liftings*, appendix to: V. B. Mehta and V. Srinivas, *Varieties in positive characteristic with trivial tangent bundle*, Compositio Math. **64** (1987), 191–212.
14. F. Oort and K. Ueno, *Principally polarized abelian varieties of dimension two or three are Jacobian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 377–381.
15. M. Rosen, *Abelian varieties over* $\mathbf{C}$, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, New York, 1986, pp. 79–101.
16. H.-G. Rück, *Abelian surfaces and Jacobian varieties over finite fields*, Compositio Math. **76** (1990), 351–366.
17. W. Scharlau, *Quadratic and Hermitian forms*, Grundlehren Math. Wiss., vol. 270, Springer-Verlag, Berlin, 1985.
18. J.-P. Serre, *Local fields*, Graduate Texts in Math., vol. 67, Springer-Verlag, New York, 1979.
19. J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki 1968/69, Lecture Notes in Math., vol. 179, Springer-Verlag, Berlin, 1971, exposé 352, pp. 95–110.
20. W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.
21. A. Weil, *Zum Beweis des Torellischen Satzes*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. IIa **1957**, 33–53.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720
Current address: Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109
E-mail address: however@math.lsa.umich.edu