

ALGEBRAIC THEORY OF COMPLEX MULTIPLICATION

1. INTRODUCTION

A natural question early in the theory of abelian varieties is whether every abelian variety in positive characteristic admits a lift to characteristic 0. That is, if A is an abelian variety over a field k with $\text{char}(k) > 0$ then does there exist a triple (R, \mathcal{A}, ϕ) consisting of a characteristic-0 local domain R with residue field k , an abelian scheme \mathcal{A} over $\text{Spec } R$, and an isomorphism ϕ from A to the special fiber \mathcal{A}_k of \mathcal{A} ; we may also wish to find (R, \mathcal{A}, ϕ) so that a specified polarization of A or subring of the endomorphism algebra of A (or both) also lifts to \mathcal{A} .

If there is an affirmative solution to such a lifting problem then general descent methods usually permit one to find a solution for which R is a complete local noetherian domain. Thus, an affirmative solution to a lifting problem as above (for a given A) is often equivalent to an appropriate deformation ring \mathcal{R} for A admitting a generic point in characteristic 0 (in which case the coordinate ring of the corresponding irreducible component of $\text{Spec } \mathcal{R}$ is such an R). If k'/k is an extension field then there is generally a natural (faithfully flat) local map $\mathcal{R} \rightarrow \mathcal{R}'$ of deformation rings, so if \mathcal{R}' has a generic point of characteristic 0 then so does \mathcal{R} . Hence, to prove an affirmative answer to such lifting questions it is usually enough to consider the case of algebraically closed k . For example, the general lifting problem for polarized abelian varieties (allowing polarizations for which the associated symmetric isogeny $A \rightarrow A^t$ is not separable) was solved affirmatively by Norman–Oort [37, Cor. 3.2] when k is algebraically closed, and from this the general case follows via deformation theory.

When a lifting problem as above has an affirmative solution, it is natural to ask if the base ring R for the lifting can be chosen to satisfy nice ring-theoretic properties, such as being normal or a discrete valuation ring. Slicing methods allow one to find an R with $\dim(R) = 1$, but unfortunately normalization generally increases the residue field. Hence, asking that the complete local noetherian domain R be normal or a discrete valuation ring with a specified residue field k is a non-trivial condition unless k is algebraically closed.

We are interested in versions of the lifting problem for finite k when we lift not only the abelian variety but also a large commutative subring of the endomorphism algebra. To avoid counterexamples it is sometimes necessary to weaken the lifting problem by permitting the initial abelian variety A to be replaced with another in the same k -isogeny class. We will precisely formulate several such lifting problems involving complex multiplication, and the main result of our work is a rather satisfactory solution to these lifting problems.

Much of the literature on complex multiplication involves either (i) working over an algebraically closed ground field, (ii) making unspecified finite extensions of the ground field, or (iii) restricting attention to simple abelian varieties. Thus, to avoid any uncertainty about

the degree of generality in which various foundational results in the theory are valid, as well as to provide a convenient reference for subsequent considerations, we begin by providing an extensive review of the algebraic theory of complex multiplication over a general base field, including special features of the theory over finite fields and over fields of characteristic 0. Then we turn our attention to the specific lifting problems which will occupy our attention for the remainder of this work.

NOTATION AND TERMINOLOGY. For a field K , we write \overline{K} to denote an algebraic closure and K_s to denote a separable closure. An extension of fields K'/K is *primary* if K is separably algebraically closed in K' . For a number field L we write \mathcal{O}_L to denote its ring of integers. If q is a power of a prime, we sometimes write \mathbb{F}_q to denote a finite field with size q (though usually we write κ or κ' to denote a finite field).

If $X \rightarrow S$ is a map of schemes and S' is an S -scheme, then $X_{S'}$ and $X_{/S'}$ denote the S' -scheme $X \times_S S'$ if S is understood from context. When $S = \text{Spec } R$ and $S' = \text{Spec } R'$ are affine, we may respectively write $X_{R'}$ or $X_{/R'}$ instead when R is understood from context. If it is necessary to specify R then we may write $X \otimes_R R'$.

For any non-zero abelian varieties A and B over a field K , $\text{Hom}(A, B)$ denotes the group of maps $A \rightarrow B$ over K , and $\text{Hom}^0(A, B)$ denotes the \mathbb{Q} -vector space $\mathbb{Q} \otimes_{\mathbb{Z}} \text{Hom}(A, B)$. When $B = A$ we write $\text{End}(A)$ and $\text{End}^0(A)$ respectively, and call $\text{End}^0(A)$ the *endomorphism algebra* of A (over K). (The endomorphism algebra is a more useful invariant than the endomorphism ring because it only depends on A up to isogeny over K .)

To avoid any possible confusion with notation found in the literature, we emphasize that what we call $\text{Hom}(A, B)$ and $\text{Hom}^0(A, B)$ are sometimes denoted by others as $\text{Hom}_K(A, B)$ and $\text{Hom}_K^0(A, B)$ (with the notation $\text{Hom}(A, B)$ and $\text{Hom}^0(A, B)$ then reserved to mean the analogues for $A_{\overline{K}}$ and $B_{\overline{K}}$ over \overline{K} , or equivalently of A_{K_s} and B_{K_s} over K_s).

We assume familiarity with the classical theory of finite-dimensional semisimple algebras over fields, including the theory of their splitting fields and maximal commutative subfields. A suitable reference for this material is [23, §4.1–4.6].

2. SIMPLICITY, ISOTYPICITY, AND ENDOMORPHISM ALGEBRAS

An abelian variety A over a field K is *simple* (over K) if it is non-zero and contains no non-zero proper abelian subvarieties. Simplicity is not generally preserved under extension of the base field; see Example 6.7 for some two-dimensional examples over finite fields and over \mathbb{Q} . The abelian variety A over K is *absolutely simple* (over K) if $A_{\overline{K}}$ is simple.

Lemma 2.1. *If A is absolutely simple over a field K then for any field extension K'/K , the abelian variety $A_{K'}$ over K' is simple.*

Proof. This is an application of direct limit and specialization arguments, as we now explain. Assume the assertion fails with some K'/K , so by replacing K' with an algebraic closure we may arrange that K is algebraically closed. Choose a non-zero proper abelian subvariety $B' \subset A_{K'}$. By expressing K' as a direct limit of finitely generated K -subalgebras, there is a finitely generated K -subalgebra $R \subset K'$ and an abelian scheme $B \rightarrow \text{Spec } R$ that is a

closed R -subgroup of A_R which descends $B' \subset A_{K'}$, so $B \rightarrow \text{Spec } R$ has fibers with constant positive dimension strictly less than $\dim(A)$. Since K is algebraically closed we can choose a K -point x of $\text{Spec } R$, and the fiber B_x is a non-zero proper abelian subvariety of A , contrary to the simplicity of A over K . ■

For a pair of abelian varieties A and B over a field K , $\text{Hom}^0(A_{K'}, B_{K'})$ can be strictly larger than $\text{Hom}^0(A, B)$ for some separable algebraic extension K'/K . For example, if E is an elliptic curve over \mathbb{Q} then considerations with the tangent line over \mathbb{Q} force $\text{End}^0(E) = \mathbb{Q}$, but it can happen that $\text{End}^0(E_L) = L$ for an imaginary quadratic field L (e.g., $E : y^2 = x^3 - x$ and $L = \mathbb{Q}(\sqrt{-1})$).

Scalar extension from number fields to \mathbb{C} or from an imperfect field to its perfect closure are useful techniques in the study of abelian varieties, so there is natural interest in considering ground field extensions that are not separable algebraic (i.e., non-algebraic or inseparable). It is an important fact that allowing such general extensions of the base field does not lead to even more maps:

Lemma 2.2 (Chow). *Let K'/K be an extension of fields that is primary. For abelian varieties A and B over K , the natural map $\text{Hom}(A, B) \rightarrow \text{Hom}(A_{K'}, B_{K'})$ is bijective.*

Proof. See [9, Thm. 3.19] for a proof using faithfully flat descent. ■

We shall be interested in certain commutative rings acting faithfully on abelian varieties, so we need some non-trivial information about the structure of endomorphism rings of abelian varieties. The study of such rings rests on the following basic result.

Theorem 2.3 (Poincaré reducibility). *Let A be an abelian variety over a field K . For any abelian subvariety $B \subset A$, there is an abelian subvariety $B' \subset A$ such that the multiplication map $B \times B' \rightarrow A$ is an isogeny.*

In particular, if $A \neq 0$ then there exist pairwise non-isogenous simple abelian varieties C_1, \dots, C_s over K such that A is isogenous to $\prod C_i^{e_i}$ for some $e_i \geq 1$.

Proof. When K is algebraically closed this result is proved in [36, §19, Thm. 1]. The same method works for perfect K , as explained in [34, Prop. 12.1]. (Perfectness is implicit in the property that the underlying reduced scheme of a finite type K -group is a K -subgroup.) The general case can be pulled down from the perfect closure via Lemma 2.2; see [9, Cor 3.20] for the argument. ■

Corollary 2.4. *For a non-zero abelian variety A over a field K and a primary extension of fields K'/K , every abelian subvariety B' of $A_{K'}$ has the form $B_{K'}$ for a unique abelian subvariety $B \subset A$.*

Proof. By the Poincaré reducibility theorem, abelian subvarieties of A are precisely the images of maps $A \rightarrow A$, and similarly for $A_{K'}$. Since scalar extension commutes with the formation of images, the assertion is reduced to the bijectivity of $\text{End}(A) \rightarrow \text{End}(A_{K'})$, which follows from Lemma 2.2. ■

Since any map between simple abelian varieties over K is either 0 or an isogeny, by general categorical arguments the collection of C_i 's (up to isogeny) in the Poincaré reducibility theorem is unique up to rearrangement, and also the multiplicities e_i are uniquely determined. We call the C_i 's in the Poincaré reducibility theorem (considered up to isogeny) the *simple factors* of A . By the uniqueness of these simple factors up to isogeny, we deduce:

Corollary 2.5. *Let A be a non-zero abelian variety A over a field, with simple factors C_1, \dots, C_s . The non-zero abelian subvarieties of A are generated by the images of maps $C_i \rightarrow A$ from the simple factors.*

By [36, §19, Thm. 3], for any two abelian varieties A and B over K , $\text{Hom}(A, B)$ is finite and free as a \mathbb{Z} -module, so $\text{Hom}^0(A, B)$ is finite-dimensional as a \mathbb{Q} -vector space. These finiteness properties rest on the following injectivity result, which is useful for many purposes.

Lemma 2.6. *Let A and B be abelian varieties over a field K . For any prime ℓ (allowing $\ell = \text{char}(K)$), the natural map*

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \text{Hom}(A, B) \rightarrow \text{Hom}(A[\ell^\infty], B[\ell^\infty])$$

is injective, where the target is the \mathbb{Z}_ℓ -module of maps of ℓ -divisible groups over K (i.e., compatible systems of maps $A[\ell^n] \rightarrow B[\ell^n]$ over K for all $n \geq 1$).

Proof. We may pass to the case when K is algebraically closed (and hence perfect). When $\ell \neq \text{char}(K)$ the assertion is a reformulation of the well-known analogous injectivity with ℓ -adic Tate modules. The proof in terms of Tate modules in [36, §19, Thm. 3] for $\ell \neq \text{char}(K)$ can be adapted to handle the case $\ell = p = \text{char}(K) > 0$ by working with the Dieudonné modules $\mathbb{D}(A[p^\infty])$ and $\mathbb{D}(B[p^\infty])$ in place of Tate modules. ■

A weakening of simplicity that is sometimes convenient is:

Definition 2.7. An abelian variety A over a field K is *isotypic* if it is isogenous to C^e for a simple abelian variety C over K and some $e \geq 1$; that is, up to isogeny, A has a unique simple factor. For a simple factor C of a non-zero abelian variety A over K , the *C -isotypic part* of A is the isotypic subvariety of A generated by the images of all maps $C \rightarrow A$. An *isotypic part* of A is a C -isotypic part for some such C .

Using the notation from the Poincaré reducibility theorem, for a non-zero abelian variety A we have

$$\text{End}^0(A) \simeq \prod \text{Mat}_{e_i}(\text{End}^0(C_i))$$

where $\{C_i\}$ is the set of simple factors of A and the e_i 's are the corresponding multiplicities. Each $\text{End}^0(C_i)$ is a division algebra, by simplicity of the C_i 's. Thus, $\text{End}^0(A)$ is always a semisimple \mathbb{Q} -algebra, it is simple if and only if A is isotypic, and it is a division algebra if and only if A is simple.

By the Poincaré reducibility theorem, every non-zero abelian variety A over a field K is naturally isogenous to the product of its distinct isotypic parts, and these distinct parts admit no non-zero maps between them. Hence, if $\{B_i\}$ is the set of isotypic parts of A then $\text{End}^0(A) = \prod \text{End}^0(B_i)$ with each $\text{End}^0(B_i)$ a simple algebra of finite dimension over \mathbb{Q} .

Explicitly, $\text{End}^0(B_i)$ is a matrix algebra $\text{Mat}_{e_i}(\text{End}^0(C_i))$ over the division algebra $\text{End}^0(C_i)$, where C_i is the unique simple factor of B_i . Beware that the composite ring map $\text{End}^0(C_i) \rightarrow \text{Mat}_{e_i}(\text{End}^0(C_i)) \simeq \text{End}^0(B_i)$ is only canonical when $\text{End}^0(C_i)$ is commutative.

In general isotypicity is not preserved by extension of the ground field. To give an example, consider a separable quadratic extension of fields K'/K and a simple abelian variety A' over K' that is not isogenous to its twist by the non-trivial element $\sigma \in \text{Gal}(K'/K)$. (For example, we can take $K = \mathbb{R}$, $K' = \mathbb{C}$, and A' an elliptic curve over \mathbb{C} with analytic model $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ for $\tau \in \mathbb{C} - \mathbb{R}$ such that $1, \tau, \bar{\tau}, \tau\bar{\tau}$ are \mathbb{Q} -linearly independent. In Example 6.8 we give examples with $K = \mathbb{Q}$.) For $A = \text{Res}_{K'/K}(A')$ we have $A_{K'} \simeq A' \times \sigma^*(A')$, so $A_{K'}$ is not isotypic and A must be simple (as otherwise a simple factor would be a K -descent of a member of the isogeny class of A' , contradicting that A' and $\sigma^*(A')$ are not isogenous). However, over finite fields there are no counterexamples:

Corollary 2.8. *If A is an isotypic abelian variety over a finite field K then $A_{K'}$ is isotypic for any finite extension K'/K .*

Proof. The key point is that for any abelian variety B' over K' and any $g \in \text{Gal}(K'/K)$, B' and $g^*(B')$ are isogenous. Indeed, since $\text{Gal}(K'/K)$ is generated by the q -Frobenius σ_q it suffices to show that B' and $\sigma_q^*(B') = B'^{(q)}$ are isogenous, and the relative q -Frobenius morphism $B' \rightarrow B'^{(q)}$ is such an isogeny. Hence, the Weil restriction $\text{Res}_{K'/K}(B')$ satisfies $\text{Res}_{K'/K}(B')_{K'} \simeq \prod_g g^*(B') \sim B'^{[K':K]}$.

Now take B' to be a simple factor of $A_{K'}$ (up to isogeny), so $\text{Res}_{K'/K}(B')$ is an isogeny factor of $\text{Res}_{K'/K}(A_{K'}) \sim A^{[K':K]}$. By simplicity of A and Poincaré reducibility it follows that $\text{Res}_{K'/K}(B')$ is isogenous to a power of A . Extending scalars, $\text{Res}_{K'/K}(B')_{K'}$ is therefore isogenous to a power of $A_{K'}$. But $B'^{[K':K]} \sim \text{Res}_{K'/K}(B')_{K'}$, so non-trivial powers of $A_{K'}$ and B' are isogenous. By simplicity of B' and Poincaré reducibility, this forces B' to be the only simple factor of $A_{K'}$ (up to isogeny). \blacksquare

3. COMPLEX MULTIPLICATION

Now we prove the fact that motivates the study of complex multiplication in the sense that we shall consider.

Theorem 3.1. *Let A be an abelian variety of dimension $g > 0$ over a field K and let $P \subset \text{End}^0(A)$ be a commutative semisimple \mathbb{Q} -subalgebra. Then $[P : \mathbb{Q}] \leq 2g$, and if equality holds then P is its own centralizer in $\text{End}^0(A)$. If moreover $P = L$ is a field of degree $2g$ over \mathbb{Q} , then A is isotypic and L is a maximal commutative subfield of $\text{End}^0(A)$.*

Proof. Consider the decomposition $P = \prod L_i$ into a product of fields. Using the primitive idempotents of P , we get a corresponding decomposition $\prod A_i$ of A in the isogeny category of abelian varieties over K , with each $A_i \neq 0$ and each L_i a commutative subfield of $\text{End}^0(A_i)$ compatibly with the inclusion $\prod \text{End}^0(A_i) \subset \text{End}^0(A)$ and the equality $\prod L_i = P$. Since $\dim(A) = \sum \dim(A_i)$, to prove that $[P : \mathbb{Q}] \leq 2g$ it suffices to treat the A_i 's separately, which is to say that we may assume that $P = L$ is a field.

Since $D = \text{End}^0(A)$ is of finite rank over \mathbb{Q} , clearly $[L : \mathbb{Q}]$ is finite. Choose a prime ℓ different from $\text{char}(K)$. The injectivity of the natural map

$$L_\ell := \mathbb{Q}_\ell \otimes_{\mathbb{Q}} L \hookrightarrow \text{End}_{\mathbb{Q}_\ell}(V_\ell(A(K_s)))$$

(see Lemma 2.6) implies that L_ℓ acts faithfully on the \mathbb{Q}_ℓ -vector space $V_\ell(A(K_s))$ of rank $2g$. But $L_\ell = \prod_{w|\ell} L_w$, where w runs over all ℓ -adic places of L , so each corresponding factor module $V_\ell(A(K_s))_w$ over L_w must be non-zero as a vector space over L_w . Hence,

$$2g \geq \sum_{w|\ell} [L_w : \mathbb{Q}_\ell] = [L : \mathbb{Q}]$$

with equality if and only if $V_\ell(A(K_s))$ is free of rank 1 over L_ℓ .

Now assume that equality holds, so $V_\ell(A(K_s))$ is free of rank 1 over L_ℓ . If A is not isotypic then by passing to an isogenous abelian variety we may arrange that $A = B \times B'$ with B and B' non-zero abelian varieties such that $\text{Hom}(B, B') = 0 = \text{Hom}(B', B)$. Hence, $\text{End}^0(A) = \text{End}^0(B) \times \text{End}^0(B')$ and so L embeds into $\text{End}^0(B)$. But $2 \dim(B) < 2 \dim(A) = [L : \mathbb{Q}]$, so we have a contradiction (since $B \neq 0$).

It remains to prove, without assuming P is a field, that if $[P : \mathbb{Q}] = 2g$ then P is its own centralizer in $\text{End}^0(A)$. (In case P is a field, so A is isotypic and hence $\text{End}^0(A)$ is simple, this clearly implies that P is a maximal commutative subfield of $\text{End}^0(A)$.) Consider once again the field decomposition $P = \prod L_i$ and the corresponding isogeny decomposition $\prod A_i$ of A as at the beginning of this proof. We have $[L_i : \mathbb{Q}] \leq 2 \dim(A_i)$ for all i , and these inequalities add up to an equality when summed over all i , so in fact $[L_i : \mathbb{Q}] = 2 \dim(A_i)$ for all i . The preceding analysis shows that each $V_\ell(A_i(K_s))$ is free of rank 1 over $L_{i,\ell} := \mathbb{Q}_\ell \otimes_{\mathbb{Q}} L_i$, and so likewise $V_\ell(A(K_s))$ is free of rank 1 over P_ℓ . Hence, $\text{End}_{P_\ell}(V_\ell(A(K_s))) = P_\ell$, so if $Z(P) \subset \text{End}^0(A)$ denotes the centralizer of P then the P_ℓ -algebra map

$$Z(P)_\ell = \mathbb{Q}_\ell \otimes_{\mathbb{Q}} Z(P) \rightarrow \text{End}_{\mathbb{Q}_\ell}(V_\ell(A(K_s)))$$

is injective (Lemma 2.6) and lands inside of $\text{End}_{P_\ell}(V_\ell(A(K_s))) = P_\ell$. In other words, the inclusion $P \subset Z(P)$ of \mathbb{Q} -algebras becomes an equality after scalar extension to \mathbb{Q}_ℓ , so $P = Z(P)$ as desired. \blacksquare

The preceding proposition justifies the interest in the following concept.

Definition 3.2. Let A be an abelian variety of dimension $g > 0$ over a field K . We say that A admits *sufficiently many complex multiplications* (over K) if there exists a commutative semisimple \mathbb{Q} -subalgebra P in $\text{End}^0(A)$ with rank $2g$ over \mathbb{Q} .

The reason for the terminology in Definition 3.2 is due to certain examples with $K = \mathbb{C}$ and P a number field such that the analytic uniformization of A expresses the P -action in terms of multiplication of certain complex numbers; see Example 5.2. The classical theory of complex multiplication focused on the case of Definition 3.2 in which P is a field, but it is useful for some purposes to allow P to be a product of several fields (i.e., a commutative semisimple \mathbb{Q} -algebra). For example, by Theorem 3.1 this is necessary if we wish to consider

the theory of complex multiplication with A that is not isotypic, or more generally if we want Definition 3.2 to be preserved under the formation of products.

Note that we do not consider A to admit sufficiently many complex multiplications merely if it does so after an extension of the base field K .

Example 3.3. The elliptic curve $y^2 = x^3 - x$ admits sufficiently many complex multiplications over $\mathbb{Q}(\sqrt{-1})$ but not over \mathbb{Q} . More generally, $\text{End}^0(E) = \mathbb{Q}$ for every elliptic curve E over \mathbb{Q} (since the tangent line at the origin is too small to support a \mathbb{Q} -linear action by an imaginary quadratic field), so we do not consider any elliptic curve over \mathbb{Q} to admit sufficiently many complex multiplications.

Proposition 3.4. *Let A be a non-zero abelian variety over a field K . The following are equivalent.*

- (1) *The abelian variety A admits sufficiently many complex multiplications.*
- (2) *Each isotypic part of A admits sufficiently many complex multiplications.*
- (3) *Each simple factor of A admits sufficiently many complex multiplications.*

See Definition 2.7 for the terminology used in (2).

Proof. Let $\{B_i\}$ be the set of isotypic parts of A , so $\text{End}^0(B_i) \simeq \text{Mat}_{e_i}(\text{End}^0(C_i))$ where C_i is the unique simple factor of B_i and $e_i \geq 1$ is its multiplicity as such. As we have already noted, $\text{End}^0(A) = \prod \text{End}^0(B_i)$. Thus, (3) implies (2), and (2) implies (1).

Conversely, assume that $\text{End}^0(A)$ contains a \mathbb{Q} -algebra $P = \prod L_i$ with fields L_1, \dots, L_s such that $\sum [L_i : \mathbb{Q}] = [P : \mathbb{Q}] = 2 \dim(A)$. We saw in the proof of Theorem 3.1 that by replacing A with an isogenous abelian variety we may arrange that $A = \prod A_i$ with each A_i a non-zero abelian variety having $L_i \subset \text{End}^0(A_i)$ compatibly with the embedding $\prod \text{End}^0(A_i) \subset \text{End}^0(A)$ and the equality $\prod L_i = P$. Thus, $[L_i : \mathbb{Q}] \leq 2 \dim(A_i)$ for all i , by Theorem 3.1, yet adding this up over all i yields an equality, so each A_i admits sufficiently many complex multiplications using L_i . Since each simple factor of A is a simple factor of some A_i , we are reduced to the case when $P = L$ is a field.

Applying Theorem 3.1 once again, L is its own centralizer in $\text{End}^0(A)$ and A is isotypic, say with unique simple factor C appearing with multiplicity e . In particular, $\text{End}^0(A) = \text{Mat}_e(D)$ for the division algebra $D = \text{End}^0(C)$ of finite degree over \mathbb{Q} . If F denotes the center of D then D is a central division algebra over F , and L must contain F since L is its own centralizer in D . Letting $d = \dim(C)$, $\text{Mat}_e(D)$ contains a maximal commutative subfield L of degree $2g/[F : \mathbb{Q}] = (2d/[F : \mathbb{Q}])e$ over F .

By the classical theory of central simple algebras over a field, all maximal commutative subfields of a rank- n^2 central simple algebra have degree n over the base field. Hence, all maximal commutative subfields of $\text{Mat}_e(D)$ have F -degree $e\sqrt{[D : F]}$, so $2d/[F : \mathbb{Q}] = \sqrt{[D : F]}$. In other words, $2d/[F : \mathbb{Q}]$ is the common F -degree of all maximal commutative subfields of $D = \text{End}^0(C)$, or equivalently $2d$ is the \mathbb{Q} -degree of all such fields. But $2d = 2 \dim(C)$, so choosing any maximal commutative subfield of D shows that C admits sufficiently many complex multiplications. ■

4. CM ALGEBRAS AND CM ABELIAN VARIETIES

The following three conditions on a number field L are easily checked to be equivalent: (i) L has no real embeddings but is quadratic over a totally real subfield, (ii) for every embedding $j : L \rightarrow \mathbb{C}$, the subfield $j(L) \subset \mathbb{C}$ is stable under complex conjugation and the involution $x \mapsto j^{-1}(\overline{j(x)})$ in $\text{Aut}(L)$ is non-trivial and independent of j , (iii) there is a non-trivial involution $\tau \in \text{Aut}(L)$ such that for every embedding $j : L \rightarrow \mathbb{C}$ we have $j(\tau(x)) = \overline{j(x)}$ for all $x \in L$. In such cases τ is unique and its fixed field is the maximal totally real subfield $L_0 \subset L$ (over which L is quadratic). The case $L_0 = \mathbb{Q}$ corresponds to the case when L is an imaginary quadratic field.

Definition 4.1. A *CM field* is a number field L satisfying the equivalent conditions (i), (ii), and (iii) above. A *CM algebra* is a product $L_1 \times \cdots \times L_s$ of finitely many CM fields (with $s \geq 1$).

The reason for this terminology is due to the following important result (along with Example 5.2).

Theorem 4.2. *Let A be an abelian variety of dimension $g > 0$ over a field K . Suppose A admits sufficiently many complex multiplications. Then there exists a CM algebra $P \subset \text{End}^0(A)$ with $[P : \mathbb{Q}] = 2 \cdot \dim(A)$. In case A is isotypic we can take P to be a CM field.*

The proof of this theorem will require some effort, especially since we consider an arbitrary base field. Before we start the proof, it is instructive to consider an example.

Example 4.3. Consider $A = E^2$ with an elliptic curve E over $K = \mathbb{C}$ such that $L := \text{End}^0(E)$ is an imaginary quadratic field. The endomorphism algebra $\text{End}^0(A) = \text{Mat}_2(L)$ is simple and contains as its maximal commutative subfields all quadratic extensions of L . Those extensions which are biquadratic over \mathbb{Q} are CM fields, and the rest are not. Hence, even when A is isotypic and $\text{char}(K) = 0$, not all maximal commutative semisimple subalgebras of $\text{End}^0(A)$ are CM algebras in general. However, if $\text{char}(K) = 0$ and A is simple (over K) then $\text{End}^0(A)$ is a CM field; see Proposition 4.7.

We will begin the proof of Theorem 4.2 now, but at a certain point we will need to use deeper input concerning the structure of endomorphism algebras of simple abelian varieties over general fields. At that point we will digress to review the required structure theory, and then we will complete the argument.

By Proposition 3.4 (and weak approximation arguments at archimedean places), to prove Theorem 4.2 it suffices to treat the case when A is simple. In this case $D = \text{End}^0(A)$ is a central division algebra over a number field F , so the commutative semisimple \mathbb{Q} -subalgebra $P \subset D$ must be a field, and the proof of Proposition 3.4 shows that the common \mathbb{Q} -degree of all maximal commutative subfields of D is $2g$. Hence, our problem is to construct a maximal commutative subfield of D that is a CM field.

Since the center F is a number field over which D is a central division algebra, there is a reduced trace map $\text{Trd}_{D/F} : D \rightarrow F$ as well as an ordinary trace map $\text{Tr}_{F/\mathbb{Q}} : F \rightarrow \mathbb{Q}$.

Let $\mathrm{Trd}_{D/\mathbb{Q}} = \mathrm{Tr}_{F/\mathbb{Q}} \circ \mathrm{Trd}_{D/F}$. Choose a polarization of A over K (as we may always do). Let $x \mapsto x^*$ denote the associated Rosati involution on D (so $(xy)^* = y^*x^*$ and $x^{**} = x$). The quadratic form $x \mapsto \mathrm{Trd}_{D/\mathbb{Q}}(xx^*)$ on D is positive-definite [36, §21, Thm. 1]. (Strictly speaking, Mumford does not work with $\mathrm{Trd}_{D/\mathbb{Q}}$, but rather with the \mathbb{Q} -trace of the multiplication map on D . However, these are positive multiples of each other.) That is, $x \mapsto x^*$ is a *positive involution* of D . This turns out to severely constrain the possibilities for D . First we record the consequences for the center.

Lemma 4.4. *The center F of $D = \mathrm{End}^0(A)$ is either totally real or a CM field, and in the latter case its canonical complex conjugation is induced by the Rosati involution defined by any polarization of A over K .*

Proof. Fix a polarization and consider the associated Rosati involution $x \mapsto x^*$ on the center F of D . The positive-definite $\mathrm{Trd}_{D/\mathbb{Q}}(xx^*)$ on D restricts to $\sqrt{[D:F]} \cdot \mathrm{Tr}_{F/\mathbb{Q}}(xx^*)$ on F , so $\mathrm{Tr}_{F/\mathbb{Q}}(xx^*)$ is positive-definite on F . If $x^* = x$ for all $x \in F$ then the rational quadratic form $\mathrm{Tr}_{F/\mathbb{Q}}(x^2)$ is positive-definite on F , so by extending scalars to \mathbb{R} we see that $\mathrm{Tr}_{(\mathbb{R} \otimes_{\mathbb{Q}} F)/\mathbb{R}}(x^2)$ is positive-definite. This forces $\mathbb{R} \otimes_{\mathbb{Q}} F$ to have no complex factors. Hence, F is a totally real field in such cases.

It remains to show that if the involution $x \mapsto x^*$ is non-trivial on F for some choice of polarization then F is a CM field and its intrinsic complex conjugation is equal to this involution on F . Let F_0 be the subfield of fixed points in F for this involution, so $[F:F_0] = 2$ and $2 \cdot \mathrm{Tr}_{F_0/\mathbb{Q}}$ is the restriction to F_0 of $\mathrm{Tr}_{F/\mathbb{Q}}$. Hence, $\mathrm{Tr}_{F_0/\mathbb{Q}}(x^2)$ is positive-definite on F_0 , so F_0 is totally real. We aim to prove that F has no real places, so we assume otherwise and seek a contradiction.

Let v be a real place of F . Since the involution $x \mapsto x^*$ is non-trivial on F and the field $F_v \simeq \mathbb{R}$ has no non-trivial field automorphisms, the real place v on F cannot be fixed by the involution $x \mapsto x^*$. Thus, the real place v^* obtained from v under the involution is a real place of F distinct from v , and so the positive-definiteness of $\mathrm{Tr}_{F/\mathbb{Q}}(xx^*)$ implies (after scalar extension to \mathbb{R}) the positive-definiteness of $\mathrm{Tr}_{(F_v \times F_{v^*})/\mathbb{R}}(xx^*)$, where $x \mapsto x^*$ on $F_v \times F_{v^*} = \mathbb{R} \times \mathbb{R}$ is the involution that swaps the factors. In other words, this is the quadratic form $(c, c') \mapsto 2cc'$, which by inspection is not positive-definite. \blacksquare

To go further with the proof of Theorem 4.2, we need to review some finer structural properties of endomorphism algebras of simple abelian varieties over arbitrary fields.

Definition 4.5. An *Albert algebra* is a pair consisting of a division algebra D of finite dimension over \mathbb{Q} and a positive involution $x \mapsto x^*$ on D .

There are non-trivial constraints on the Albert algebras that arise from polarized simple abelian varieties A over an arbitrary field K . Before listing these constraints, it is convenient to first record Albert's classification of general Albert algebras (omitting the description of the possibilities for the involution).

Theorem 4.6 (Albert). *Let $(D, (\cdot)^*)$ be an Albert algebra, and for any place v of the center F let v^* denote the pullback of v along the involution. Exactly one of the following occurs:*

Type I: $D = F$ is a totally real field.

Type II: D is a central quaternion division algebra over a totally real field F such that D splits at each real place of F .

Type III: D is a central quaternion division algebra over a totally real field F such that D is non-split at each real place of F .

Type IV: D is a central division algebra over a CM field F such that D splits at all finite places v of F for which $v = v^*$ and $\text{inv}_v(D) + \text{inv}_{v^*}(D) = 0$ in \mathbb{Q}/\mathbb{Z} for all finite places v of F .

Proof. See [36, §21, Thm. 2] (which also records the possibilities for the involution). ■

Let A be a simple abelian variety over a field K , $D = \text{End}^0(A)$, and F the center of D . Let F_0 be the maximal totally real subfield of F , so either $F = F_0$ or F is a totally imaginary quadratic extension of F_0 . The invariants $e = [F : \mathbb{Q}]$, $e_0 = [F_0 : \mathbb{Q}]$, $d = \sqrt{[D : F]}$, and $g = \dim(A)$ must satisfy some divisibility restrictions:

- the action of the endomorphism algebra on rational homology when $K = \mathbb{C}$ (not needing simplicity!) implies via the Lefschetz Principle that $ed^2 = [D : \mathbb{Q}]$ divides $2g$ when $\text{char}(K) = 0$,
- the action of D on $V_\ell(A(K_s))$ with $\ell \neq \text{char}(K)$ implies (via [36, §19, Cor. to Thm. 4], whose proof is valid over any base field) that $ed|2g$ for any K ,
- the structure of symmetric elements in $\mathbb{Q} \otimes_{\mathbb{Z}} \text{Hom}(A, A^t) \simeq \mathbb{Q} \otimes_{\mathbb{Z}} \text{Pic}(A)/\text{Pic}^0(A)$ (via [36, §20, Cor. to Thm. 3], whose proof is valid over any base field) yields that $[F' : \mathbb{Q}]|g$ for every commutative subfield $F' \subset D$ whose elements are invariant under the involution.

The results are summarized in the following table, taken from the end of [36, §21]. (As we have just observed, the hypothesis there that K is algebraically closed is not necessary). The invariants of $D = \text{End}^0(A)$ are given in the first three columns. In the last two columns we give some necessary restrictions on these invariants.

Type	e	d	$\text{char}(K) = 0$	$\text{char}(K) > 0$
I	$e = e_0$	1	$e g$	$e g$
II	$e = e_0$	2	$2e g$	$2e g$
III	$e = e_0$	2	$2e g$	$e g$
IV	$e = 2e_0$	d	$e_0 d^2 g$	$e_0 d g$

For example, in the case of Type II (in any characteristic) we have $\mathbb{R} \otimes_{\mathbb{Q}} D = (\mathbb{R} \otimes_{\mathbb{Q}} F) \otimes_F D = \prod_{v|\infty} F_v \otimes_F D \simeq \text{Mat}_2(F_v)^e$, and by [36, §21, Thm. 2] it can be arranged that the positive involution on D goes over to transpose on each $\text{Mat}_2(F_v) = \text{Mat}_2(\mathbb{R})$. Thus, for D of

Type II the fixed part of the involution on D has \mathbb{Q} -dimension $2e$ and hence F -degree 2. By centrality of F in the division algebra D , the condition $x^* = x$ for x in D of Type II therefore defines a necessarily commutative quadratic extension F' of F inside of D , so g is divisible by $[F' : \mathbb{Q}] = 2e$.

We refer the reader to [41] for further information on these invariants. Using this table, we can prove the following additional facts when the simple A admits sufficiently many complex multiplications.

Proposition 4.7. *Let A be a simple abelian variety of dimension $g > 0$ over a field K , and assume that A admits sufficiently many complex multiplications. Let $D = \text{End}^0(A)$.*

- (1) *If $\text{char}(K) = 0$ then D is of Type IV with $d = 1$ and $e = 2g$.*
- (2) *If $\text{char}(K) > 0$ then D is of Type III or Type IV.*

Proof. First suppose $\text{char}(K) = 0$. Let $P \subset D$ be a commutative semisimple \mathbb{Q} -subalgebra with $[P : \mathbb{Q}] = 2g$. Since D is a division algebra, P is a field. The table says that the $[D : \mathbb{Q}] = ed^2$ divides $[P : \mathbb{Q}] = 2g$, so the inclusion $P \subset D$ is an equality. Thus, D is commutative (i.e., $d = 1$), so $D = F$ is a commutative field and hence $e := [F : \mathbb{Q}] = 2g$ by the complex multiplication hypothesis. But the table shows that in characteristic 0 we have $e|g$ for Types I, II, and III, so D must be of Type IV.

Now suppose $\text{char}(K) > 0$. In view of the divisibility relations in the table in positive characteristic, D cannot be of Type I since in such cases D is a commutative field whose \mathbb{Q} -degree divides $\dim(A)$, contradicting the existence of sufficiently many complex multiplications. Likewise, in case of Type II we have $2e|g$ yet $2e = 2[F : \mathbb{Q}]$ is the \mathbb{Q} -degree of a maximal commutative subfield of the central quaternion division algebra D over F , so there are no such subfields with \mathbb{Q} -degree $2g$. Since a commutative semisimple \mathbb{Q} -subalgebra of D must be a field (as D is a division algebra), Type II is not possible if the simple A has sufficiently many complex multiplications. ■

Finally, we can complete the proof of Theorem 4.2. Proposition 4.7(1) settles the case of characteristic 0, and Proposition 4.7(2) gives that $D = \text{End}^0(A)$ is an Albert algebra of Type III or IV when $\text{char}(K) > 0$. If D is of Type III then the center F is totally real and d is even, whereas if D is of Type IV then F is CM. Thus, we can apply the following general lemma to conclude the proof.

Lemma 4.8 (Tate). *Let D be a central division algebra of degree d^2 over a number field F that is totally real or CM. If F is totally real then assume that d is even. There exists a maximal commutative subfield $L \subset D$ that is a CM field.*

The parity condition on d is necessary when F is totally real, since $d = [L : F]$ by maximality of L in D .

Proof. By the theory of central simple algebras, any degree- d extension of F that splits D is a maximal commutative subfield of D . Hence, we just need to find a degree- d extension L of F that is a CM field and splits D . There is a finite non-empty set Σ of finite places of

F containing the finite places at which D is non-split, and by the theory of Brauer groups of local fields we know that D is split by any extension of F_v of degree d for any $v \in \Sigma$.

First assume that F is totally real, so d is even. By weak approximation, there is a monic polynomial f over F of degree $d/2$ that is close to an irreducible one over F_v for all $v \in \Sigma$ (and in particular f is irreducible over all such F_v , and hence over F since Σ is non-empty). We can also arrange that for each real place v of F the polynomial f viewed over $F_v \simeq \mathbb{R}$ is close to a totally split polynomial and hence is totally split over F_v . Thus, $F' = F[x]/(f)$ is a totally real extension of F with degree $d/2$. By the same method, we can construct a quadratic extension L/F' that is unramified quadratic over each place v' over a place in Σ and is totally complex (by using approximations to irreducible quadratics over \mathbb{R} at the real places of F'). This L is a CM field and it is designed so that $F_v \otimes_F L$ is a degree- d field extension of F_v for all $v \in \Sigma$, so D_L is split at all places of L (the archimedean ones being obvious). Hence, D_L is split over L .

Now assume that F is a CM field. Let $F_0 \subseteq F$ be the maximal totally real subfield. By the same weak approximation procedure as above (replacing $d/2$ with d), we can construct a degree d totally real extension F'_0/F_0 such that for each place v_0 of F_0 beneath a place $v \in \Sigma$, the extension F'_0/F_0 has a unique place v'_0 over v_0 with $(F'_0)_{v'_0}/(F_0)_{v_0}$ totally ramified when F'_0/F_0 is unramified at v'_0 and unramified when F'_0/F_0 is ramified at v'_0 . Hence, $(F'_0)_{v'_0}$ and F_v are linearly disjoint over $(F_0)_{v_0}$. We conclude that F'_0 and F are linearly disjoint over F' , so $L := F'_0 \otimes_{F'_0} F$ is a field and each $v \in \Sigma$ has a unique place w over it in L with $[L_w : F_v] = d$. Thus, L splits D . By construction, L is visibly CM. ■

Corollary 4.9. *An isotypic abelian variety A with sufficiently many complex multiplications remains isotypic after any extension of the base field.*

Proof. By Theorem 4.2, $\text{End}^0(A)$ contains a commutative field with \mathbb{Q} -degree $2 \dim(A)$. This property is preserved after any ground field extension (even though the endomorphism algebra may get larger), so by the final part of Theorem 3.1 isotypicity is preserved as well. ■

It turns out to be convenient to view the CM algebra P in Theorem 4.2 as an abstract ring in its own right, and to thereby regard the embedding $P \hookrightarrow \text{End}^0(A)$ as additional structure on A . This is encoded in the following concept.

Definition 4.10. Let A be an abelian variety over K with sufficiently many complex multiplications, and $j : P \hookrightarrow \text{End}^0(A)$ an embedding of a CM algebra P with $[P : \mathbb{Q}] = 2 \dim(A)$. Such a pair (A, j) is called a *CM abelian variety* (with complex multiplication by P).

It must be emphasized that in this definition we are requiring P to be embedded in the endomorphism algebra of A over K (and not merely in the endomorphism algebra after an extension of K). For example, according to this definition, no elliptic curve over \mathbb{Q} admits a structure of CM elliptic curve (even if such a structure exists after an extension of the base field).

We end this section by giving a more precise result concerning the possibilities for F in case of Type III in Proposition 4.7(2). This will not be used later:

Proposition 4.11. *Let A , K , and D be as in Proposition 4.7(2), and let F be the center of D , $g = \dim(A)$, $d = \sqrt{[D : F]}$, and $e = [F : \mathbb{Q}]$. We have $ed = 2g$, and if D is of Type III (so $d = 2$) then either $F = \mathbb{Q}$ or $F = \mathbb{Q}(\sqrt{p})$.*

Proof. Since we are in Type III, F is totally real. By direct limit considerations, we can descend to the case when K is finitely generated over \mathbb{F}_p , and then identify A with the generic fiber of an abelian scheme $\mathcal{A} \rightarrow S$ of relative dimension g over an integral \mathbb{F}_p -scheme S of finite type with function field K . By shrinking S , we can arrange that $\text{End}(A) = \text{End}(\mathcal{A})$, so we have specialization maps $D = \text{End}^0(A) \rightarrow \text{End}^0(\mathcal{A}_s)$ for every closed point $s \in S$. These are injective due to the identification of ℓ -power torsion in all geometric fibers for a prime $\ell \neq p$. In fact, since the $\mathcal{A}[\ell^n]$'s are finite étale over S , the representation of $\text{Gal}(K_s/K)$ on $V_\ell(A(K_s))$ factors through the quotient $\pi_1(S, \eta)$, where $\eta : \text{Spec}(K_s) \rightarrow S$ is the geometric generic point.

By Theorem 4.2, we can choose a CM field $L \subset D$ with $[L : \mathbb{Q}] = 2g$. In particular, L embeds into $\text{End}^0(\mathcal{A}_s)$ with $[L : \mathbb{Q}] = 2g = 2 \dim(\mathcal{A}_s)$, so each \mathcal{A}_s is isotypic. By Theorem 3.1, L is its own centralizer in $\text{End}^0(\mathcal{A}_s)$, so the central Frobenius endomorphism $\varphi_s \in \text{End}^0(\mathcal{A}_s)$ lies in the image of L and hence lifts into a central element of $\text{End}^0(A)$. Thus, we get a subfield Z of F generated by the lifts of the φ_s 's as s varies through all closed points of S . In particular, $\mathbb{Q}[\varphi_s]$ is a totally real field since F is totally real. But by Weil's Riemann Hypothesis for abelian varieties over finite fields (see the discussion following Definition 6.2), under any embedding $\iota : \mathbb{Q}[\varphi_s] \hookrightarrow \mathbb{C}$ we have each $\iota(\varphi_s)\overline{\iota(\varphi_s)} = q_s$ for $q_s = \#\kappa(s) \in p^{\mathbb{Z}}$, so the real number $\iota(\varphi_s)$ is a power of \sqrt{p} . Hence, the subfield $\mathbb{Q}[\varphi_s] \subset F$ is either \mathbb{Q} or $\mathbb{Q}(\sqrt{p})$, so the subfield $Z \subset F$ is either \mathbb{Q} or $\mathbb{Q}(\sqrt{p})$.

Choose a prime $\ell \neq p$. By the Chebotarev Density Theorem for $\pi_1(S, \eta)$, the Frobenius elements at the closed points of S generate a dense subgroup, so the subalgebra $Z_\ell := \mathbb{Q}_\ell \otimes_{\mathbb{Q}} Z \subset \text{End}_{\mathbb{Q}_\ell}(V_\ell(A(K_s)))$ is equal to the image of $\mathbb{Q}_\ell[\text{Gal}(K_s/K)]$. Thus, we have an injective map

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} D \hookrightarrow \text{End}_{\mathbb{Q}_\ell[\text{Gal}(K_s/K)]}(V_\ell(A(K_s))) = \text{End}_{Z_\ell}(V_\ell(A(K_s))).$$

By Zarhin's theorem [56] (see [35, XII, §2] for a proof allowing $p = 2$) this injection is an isomorphism, so we conclude that F_ℓ is central in $\text{End}_{Z_\ell}(V_\ell(A(K_s)))$. But the center of this latter algebra is Z_ℓ , so the inclusion $Z_\ell \subset F_\ell$ is an equality. Hence, the inclusion $Z \subset F$ is an equality as well. Since Z is either \mathbb{Q} or $\mathbb{Q}(\sqrt{p})$, we are done. \blacksquare

5. CM TYPES

Let A be an isotypic abelian variety of dimension $g > 0$ over a field K such that A admits sufficiently many complex multiplications. By Theorem 4.2, we may and do choose a CM field $L \subset \text{End}^0(A)$ with degree $2g$. It turns out that the L -linear isogeny class of A is encoded in terms of a rather simple discrete invariant when $\text{char}(K) = 0$. We wish to review the basic features of this invariant, called the CM type, and to discuss some useful replacements for it in positive characteristic.

The order $\mathcal{O} = L \cap \text{End}(A)$ in L acts on A over K , so $\mathcal{O} \otimes_{\mathbb{Z}} K$ acts K -linearly on the tangent space $T = T_0(A)$. Hence, if $\text{char}(K) = 0$ then $L = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ acts K -linearly on T , whereas if $\text{char}(K) = p > 0$ then $\mathcal{O}/(p)$ acts K -linearly on T . In particular, if $\text{char}(K) = 0$ then the isomorphism class of the $L \otimes_{\mathbb{Q}} K$ -module T is an invariant of the L -linear isogeny class of A over K , whereas nothing of the sort is true when $\text{char}(K) = p > 0$.

We now focus on the case $\text{char}(K) = 0$. Let F/K be an algebraically closed extension. Since $L \otimes_{\mathbb{Q}} K$ is a product of finitely many finite extensions of K (all separable over K), the isomorphism class of an $L \otimes_{\mathbb{Q}} K$ -module with finite K -dimension is determined by the isomorphism class of the $L \otimes_{\mathbb{Q}} F$ -module obtained by scalar extension from K to F . The F -algebra $L \otimes_{\mathbb{Q}} F$ has a very simple form: it is $\prod_{\varphi} F_{\varphi}$ where φ ranges through all field embeddings $L \rightarrow F$ and F_{φ} denotes F viewed as an L -algebra via φ . Hence, any $L \otimes_{\mathbb{Q}} F$ -module M decomposes into a corresponding product of eigenspaces M_{φ} over F on which L acts through φ . We conclude that for an $L \otimes_{\mathbb{Q}} K$ -module M with finite K -dimension, the isomorphism class of M is determined by the numbers $\dim_F(M \otimes_K F)_{\varphi}$ as φ varies through $\text{Hom}(L, F)$.

On the set $\text{Hom}(L, F) = \text{Hom}(L, \overline{\mathbb{Q}})$ (with $\overline{\mathbb{Q}}$ the algebraic closure of \mathbb{Q} in F) there is a natural involution defined by precomposition with the intrinsic complex conjugation ι of the CM field L (i.e., the non-trivial automorphism of L over its maximal totally real subfield L_0). This decomposes the set $\text{Hom}(L, F)$ of size $2g$ into g ‘‘conjugate pairs’’ of embeddings. In the special case $F = \mathbb{C}$ we can also compute the involution on $\text{Hom}(L, F)$ by using composition with complex conjugation on $F = \mathbb{C}$.

In the motivating example of the $L \otimes_{\mathbb{Q}} F$ -module $M = T \otimes_K F$ arising from a CM abelian variety over K with complex multiplication by L , there is a non-trivial constraint on the L -eigenspaces of $T \otimes_K F$: each eigenspace is a line, and if Φ denotes the set of g distinct embeddings $\varphi : L \rightarrow F$ for which there is a φ -eigenline in $T \otimes_K F$ then Φ contains no ‘‘conjugate pairs’’. That is, we have a disjoint union decomposition $\text{Hom}(L, F) = \bigsqcup (\Phi \circ \iota)$. To prove these properties of the L -action on $T \otimes_K F$ when $\text{char}(K) = 0$, we first note that the choice of algebraically closed extension F/K does not matter and so it suffices to treat the case when K is finitely generated over \mathbb{Q} . We may then reduce to the case $K = F = \mathbb{C}$ (using the last part of Proposition 3.1 to see preservation of isotypicity), in which case a proof is given via the complex-analytic uniformization in [36, §22]. These considerations lead us to make:

Definition 5.1. Let L be a CM field and F an algebraically closed field of characteristic 0. An F -valued *CM type* for L is a subset $\Phi \subset \text{Hom}(L, F)$ of representatives for the g orbits of the action by the complex conjugation ι of L . That is, Φ consists of g distinct elements such that $\varphi \circ \iota \notin \Phi$ for all $\varphi \in \Phi$.

The preceding discussion shows that if K is a field of characteristic 0 and F/K is an algebraically closed extension, then the tangent space to a CM abelian variety A over K with complex multiplication by L determines an F -valued CM type Φ for L . This is an invariant of the L -linear isogeny class of A over K .

In general the CM type takes values in the algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} in F , so if we first choose this latter algebraic closure and then take F to be equipped with a specified embedding of this $\overline{\mathbb{Q}}$ then we can regard the CM type as being independent of F ; this is sometimes useful for passing between different choices of F (such as \mathbb{C} and $\overline{\mathbb{Q}_p}$).

Example 5.2. Let L be a CM field and Φ a \mathbb{C} -valued CM type on L . Let $(\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi}$ denote $\mathbb{R} \otimes_{\mathbb{Q}} L = \prod_{v|\infty} L_v$ endowed with the complex structure defined via the isomorphism $L_v \simeq \mathbb{C}$ using the unique element $\varphi_v \in \Phi$ pulling back the standard absolute value of \mathbb{C} to the place v of L for each $v|\infty$. In other words, $(\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi} = \prod_{\varphi \in \Phi} \mathbb{C}_{\varphi}$ where \mathbb{C}_{φ} denotes \mathbb{C} equipped with the L -action via $\varphi : L \rightarrow \mathbb{C}$. We view the ring of integers \mathcal{O}_L as a lattice in $\mathbb{R} \otimes_{\mathbb{Q}} L = \mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_L$ in the natural way, so the quotient $(\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi} / \mathcal{O}_L$ is a complex torus of dimension $[L : \mathbb{Q}] / 2$.

In the complex-analytic theory [36, §22] it is proved (using that L is a CM field) that this complex torus admits a Riemann form and hence is an abelian variety. Let A_{Φ} be the corresponding abelian variety over \mathbb{C} . By construction, there is an action by \mathcal{O}_L on A_{Φ} and hence an embedding $L \hookrightarrow \text{End}^0(A_{\Phi})$ as a subfield of \mathbb{Q} -degree $[L : \mathbb{Q}] = 2 \dim(A_{\Phi})$. This makes A_{Φ} into a CM abelian variety over \mathbb{C} with complex multiplication by L , and the action by any $c \in \mathcal{O}_L \subset \text{End}(A_{\Phi})$ is expressed on the tangent space $(\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi} = \prod_{\varphi \in \Phi} \mathbb{C}_{\varphi}$ as the map $c \cdot (a_{\varphi}) = (\varphi(c)a_{\varphi})$ involving multiplication in \mathbb{C} . In particular, A_{Φ} equipped with the embedding $L \hookrightarrow \text{End}^0(A_{\Phi})$ gives rise to the CM type Φ on L .

The CM abelian varieties A_{Φ} are generally not simple, and it is shown in the classical theory [36, §22, First Ex., Thm.] that as we vary Φ through all CM types on L , the A_{Φ} 's vary (without repetition) through all L -linear isogeny classes of (necessarily isotypic) CM abelian varieties over \mathbb{C} with complex multiplication by L .

Since we may make the CM type essentially be independent of F by replacing F with $\overline{\mathbb{Q}}$, we can deduce the following purely algebraic consequence:

Proposition 5.3. *Let K be an algebraically closed field of characteristic 0. Let L be a CM field, and consider CM abelian varieties A over K with complex multiplication via $j : L \hookrightarrow \text{End}^0(A)$. The L -linear isogeny class of such an A is uniquely determined by the K -valued CM type Φ on L associated to (A, j) , and every CM type on L arises in this way.*

Proof. In view of Lemma 2.2, by direct limit arguments we can reduce to the case when the base field has finite transcendence degree over \mathbb{Q} . To show that the CM type determines the L -linear isogeny class it suffices (again by Lemma 2.2) to treat the case $K = \mathbb{C}$. This case was addressed in Example 5.2 via the complex-analytic theory, where it was also seen that every CM type Φ on L does arise when $K = \mathbb{C}$.

It remains to show that every CM type Φ on L arises when $K = \overline{\mathbb{Q}}$. Consider the CM abelian variety A_{Φ} over \mathbb{C} with complex multiplication by L and CM type Φ as in Example 5.2. Recall that $\mathcal{O}_L = L \cap \text{End}(A_{\Phi})$. By expressing \mathbb{C} as a direct limit of its finitely generated $\overline{\mathbb{Q}}$ -subalgebras, there is such a subalgebra R for which A with its \mathcal{O}_L -action descends to an abelian scheme over R equipped with an \mathcal{O}_L -action. By localization of R , we can arrange that the tangent space to the abelian scheme is a finite free R -module, and by increasing R to contain the integer ring of the Galois closure of L in \mathbb{C} we can arrange that the \mathcal{O}_L -action

on the tangent space decomposes according to Φ . Now specializing at a maximal ideal of R gives the required example over \mathbb{Q} . \blacksquare

This proposition has an important consequence for descending the field of definition of a CM abelian variety in characteristic 0, as we will see in Theorem 7.3.

Remark 5.4. By Theorem 3.1, any abelian variety A as in Proposition 5.3 has a unique simple factor C . By Proposition 3.4, this simple factor C is a CM abelian variety with complex multiplication by the CM field $L' := \text{End}^0(C)$ (see Proposition 4.7(1)). Since L' is canonically identified with the center of $\text{End}^0(A)$, it naturally embeds into L . Hence, there is an F -valued CM type Ψ on L' arising from C , and the pair (L', Ψ) is determined by (L, Φ) since A with its complex multiplication by L is determined up to L -linear isogeny by Φ (and $L' = L$ if and only if $A = C$, which is to say that A is simple). It is therefore natural to seek an intrinsic recipe to directly construct (L', Ψ) from (L, Φ) , and in particular to characterize in terms of Φ whether or not A is simple. Since the base field F is algebraically closed, it suffices to treat the case $F = \mathbb{C}$, and in this case such a recipe is provided by the complex-analytic theory: among the CM fields in L from which Φ is obtained by full preimage under restriction, (L', Ψ) is the unique such pair with $[L' : \mathbb{Q}]$ minimal and Φ the full preimage of Ψ .

In positive characteristic a good concept of CM type does not really exist, since the tangent space has no action by L but only by the order $\mathcal{O} = L \cap \text{End}(A)$. More specifically, if $\text{char}(K) = p > 0$ then T has a K -linear action by $\mathcal{O}/(p)$ and there is generally no constraint on this action akin to the eigenspace decomposition considered in characteristic 0. The lack of such a constraint occurs for a couple of reasons, as we now explain.

First of all, if p is not totally inert in L or divides the discriminant of \mathcal{O} over \mathbb{Z} then $\mathcal{O}/(p)$ fails to be a field. In such cases there is no notion of eigenspace decomposition which closely resembles the situation in characteristic 0.

Suppose instead that \mathcal{O} has discriminant not divisible by p and p is totally inert in L . In such cases $\kappa := \mathcal{O}/(p)$ is a finite field of degree $2g$ over \mathbb{F}_p and $\text{Aut}(L/\mathbb{Q})$ injects into $\text{Gal}(\kappa/\mathbb{F}_p)$, so complex conjugation on L induces a non-trivial involution on κ . For an algebraically closed extension F/K we can consider the eigenspace decomposition of $T \otimes_K F$ over $\kappa \otimes_{\mathbb{F}_p} F = \prod_{\varphi} F_{\varphi}$ where φ ranges over the $2g$ distinct embeddings of κ into F . This could fail to resemble the CM types that arise in characteristic 0 because (as we shall see in later examples) there may be conjugate pairs occurring among the φ 's for which $T \otimes_K F$ has a non-zero φ -eigenspace for its κ -action. In such cases, the composite action

$$\mathcal{O} \rightarrow \text{End}(A) \rightarrow \text{End}(A)/(p) \rightarrow \text{End}_K(T)$$

does not “look like the reduction of a CM type”, and so this provides an obstruction for A equipped with its \mathcal{O} -action to lift to characteristic 0. (The possibility that for some φ the φ -eigenspace in $T \otimes_K F$ has F -dimension larger than 1 cannot occur. Indeed, the Dieudonne module $D := \mathbb{D}(A_F[p^\infty])$ must be free of rank 1 over $\mathcal{O}_L \otimes_{\mathbb{Z}} W(F)$ due to Lemma 2.6 and $W(F)$ -rank considerations, and $T \otimes_K F \simeq D/\phi(D)$ as $\kappa \otimes_{\mathbb{F}_p} F$ -modules with $\phi : D \rightarrow D$ the semilinear Frobenius endomorphism. Hence, $T \otimes_K F$ is monogenic over $\kappa \otimes_{\mathbb{F}_p} F$.)

An obstruction of this sort to the existence of a CM-lift in characteristic 0 will be formulated precisely later, and will be used to exhibit examples of abelian varieties over finite fields which do not admit a lifting to characteristic 0 with sufficiently many complex multiplications. This is interesting due to Corollary 6.6 below, according to which *every* abelian variety over a finite field admits sufficiently many complex multiplications. The above obstruction to lifting such abelian varieties to characteristic 0 along with the action of a large CM algebra is also useful in the search for another member of the isogeny class that might admit such a lifting.

Since the tangent space fails to be an isogeny invariant for the study of CM abelian varieties in positive characteristic (and $\text{End}^0(A)$ does not act on the tangent space when $\text{char}(K) > 0$), there is an alternative linear object attached to a CM abelian variety that serves as a good substitute when $\text{char}(K) = p > 0$: the p -divisible group. This rests on Lemma 2.6, as follows. Taking $B = A$ in Lemma 2.6, we see that $\mathbb{Z}_p \otimes_{\mathbb{Z}} \text{End}(A)$ acts faithfully on $\text{End}(A[p^\infty])$. Hence, $\mathbb{Q}_p \otimes_{\mathbb{Q}} \text{End}^0(A)$ acts faithfully on $A[p^\infty]$ in the isogeny category of p -divisible groups over K . In particular, if K is perfect (e.g., finite) and A is an isotypic CM abelian variety over K with complex multiplication by the CM field L then $L_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} L$ acts faithfully and linearly on the vector space $\mathbb{D}(A[p^\infty])[1/p]$ of rank $2g$ over the absolutely unramified p -adic field $W(K)[1/p]$. This viewpoint will be useful in some later considerations with lifting problems from positive characteristic to characteristic 0, and it is an analogue for the action by L on the filtered K -vector space $H_{\text{dR}}^1(A/K)$ of dimension $2g$ when $\text{char}(K) = 0$ (providing essentially the same information as the CM type arising from the L -action on $T_0(A) = H^0(A, \Omega_{A/K}^1)^*$.)

6. ABELIAN VARIETIES OVER FINITE FIELDS

We now assume that $K = \kappa$ is a finite field with $\text{char}(\kappa) = p$. A fundamental fact in the theory of abelian varieties over finite fields is Tate's *isogeny theorem*:

Theorem 6.1 (Tate). *Let A be an abelian variety over a finite field κ . The injective map in Lemma 2.6 is bijective for all primes ℓ .*

Proof. The case $\ell \neq \text{char}(\kappa)$ is the main result in [49]; it is also proved in [36, App. I, Thm. 1]. Unfortunately, Tate did not publish his proof for the case $\ell = p$. This proof is given in [33] (and see [15, §8] for an alternative exposition using less non-commutative algebra). ■

Tate's proof of his isogeny theorem is closely tied up with his analysis of the general structure of endomorphism algebras of abelian varieties over finite fields. The essential case, and the one on which we will now focus, is a simple abelian variety A over a finite field κ . In this case $D := \text{End}^0(A)$ is a division algebra of finite dimension over \mathbb{Q} . If $q = \#\kappa$ then the q -Frobenius endomorphism

$$\pi_A = \pi : A \longrightarrow A$$

is central in D since the q -Frobenius is functorial for all κ -schemes. Hence, the number field $\mathbb{Q}[\pi] = \mathbb{Q}(\pi)$ is contained in the center of D . Tate proved, even without simplicity or

isotypicity hypotheses on A , that $\mathbb{Q}[\pi]$ is the center of $\text{End}^0(A)$ for any abelian variety A over κ [36, Thm. 3(a)].

Definition 6.2. In a field of characteristic 0, a *Weil q -number* is an algebraic integer all of whose \mathbb{Q} -conjugates in \mathbb{C} have absolute value $q^{1/2}$.

The interest in Definition 6.2 is because Weil proved that for any (non-zero) abelian variety A over κ and any $\ell \neq p := \text{char}(\kappa)$, the \mathbb{Q}_ℓ -linear q -Frobenius action on $V_\ell(A(\kappa_s))$ is a polynomial $f_{A,q} \in \mathbb{Z}[T]$ that is independent of ℓ and has all roots in \mathbb{C} equal to Weil q -numbers. (See [43, §3].) In the special case that A is a simple abelian variety over κ , it follows that under any embedding $F := \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, the effect of complex conjugation on F is characterized by the intrinsic formula $\pi \mapsto q/\pi$. Hence, F is either totally real (with $\pi^2 = q$) or a CM field, recovering Lemma 4.4 in the special case of finite base fields. In particular, when F is totally real the only possibilities for F are \mathbb{Q} (when $q = p^n$ with n even) and $\mathbb{Q}(\sqrt{p})$ (when $q = p^n$ with n odd).

Tate's isogeny theorem implies some non-trivial results concerning the splitting behavior of the central division algebra $D = \text{End}^0(A)$ over F (with A simple over κ), as follows. Since π encodes the action of the topological q -Frobenius generator of $\text{Gal}(\kappa_s/\kappa)$ on any ℓ -adic Tate module of A for $\ell \neq p$, the isogeny theorem gives an F_ℓ -linear isomorphism

$$F_\ell \otimes_F D \simeq \text{End}_{F_\ell}(V_\ell(A(\kappa_s))),$$

where $F_\ell = \mathbb{Q}_\ell \otimes_{\mathbb{Q}} F = \prod_{v|\ell} F_v$. Passing to F_v -components for $v|\ell$, this implies that D is split at all places of F away from real and p -adic places. The splitting behavior at the real and (especially) p -adic places is rather more subtle, and this was completely worked out by Tate; see [49], [51, Thm. 1], and [43, §5] for further discussion about the structure of the central division algebra D over F .

In Tate's work, he also proved [36, App. I, Thm. 3(e)] that A is isotypic if and only if the common characteristic polynomial $f_{A,q} \in \mathbb{Z}[T]$ of the q -Frobenius action on the Tate modules has a single monic irreducible factor over \mathbb{Q} , in which case this irreducible factor is obviously the minimal polynomial f_π over \mathbb{Q} for the q -Frobenius endomorphism $\pi \in \text{End}^0(A)$. (Recall that $\mathbb{Q}[\pi]$ is the center of $\text{End}^0(A)$.) The polynomial f_π only depends on A through its isogeny class (due to the functoriality of q -Frobenius on κ -schemes), and by Weil its $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -conjugacy class of roots in \mathbb{C} consists of Weil q -numbers.

Now fix an algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} and let $W(q)$ denote the set of Weil q -numbers in $\overline{\mathbb{Q}}$. We wish to consider elements of $W(q)$ to be equivalent when they lie in the same $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbit, or in other words they have the same minimal polynomial over \mathbb{Q} . The following remarkable result, whose proof ultimately uses mod- p reduction of descents to number fields of CM abelian varieties over \mathbb{C} , relates Weil q -numbers to isogeny classes of simple abelian varieties over a finite field of size q .

Theorem 6.3 (Honda–Tate). *Let κ be a finite field of size q . The assignment $A \mapsto \pi_A$ defines a bijection from the set of isogeny classes of simple abelian varieties over κ to the set of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -conjugacy classes of Weil q -numbers.*

We refer the reader to [22], [51], [15], and [43] for a discussion of the proof of the Honda–Tate theorem, where the following consequence of the proof of the Honda–Tate theorem is also addressed, describing the possibilities for the division algebra $\text{End}^0(A)$ depending on whether the center F is \mathbb{Q} , $\mathbb{Q}(\sqrt{p})$ (the totally real cases), or a CM field.

Corollary 6.4. *Let A be a simple abelian variety over a finite field κ of size q and characteristic p . Let $D = \text{End}^0(A)$, $\pi \in D$ the q -Frobenius endomorphism, and $F = \mathbb{Q}(\pi)$ the center of D . Exactly one of the following occurs.*

- (1) *We have $\pi^2 = q = p^n$ with n even. This is precisely the case $F = \mathbb{Q}$, and occurs exactly when D is a central quaternion division algebra over \mathbb{Q} , in which case it is the unique quaternion division algebra over \mathbb{Q} ramified at exactly p and at ∞ . The corresponding isogeny class of simple abelian varieties consists of supersingular elliptic curves over κ whose geometric endomorphism algebra is defined over κ .*
- (2) *We have $\pi^2 = q = p^n$ with n odd. This is precisely the case $F = \mathbb{Q}(\sqrt{p})$, and occurs exactly when D is the unique central quaternion division algebra over F ramified at exactly the two infinite places of F . The corresponding isogeny class of simple abelian varieties is represented by the 2-dimensional Weil restriction $\text{Res}_{\kappa'/\kappa}(E')$ where κ'/κ is a quadratic extension and E' is a supersingular elliptic curve over κ' whose geometric endomorphism algebra is not defined over κ' .*
- (3) *The field F is a CM field. In such cases, D is the central division algebra over F that is split at all places of F away from p and for each p -adic place v of F has local invariant $\text{inv}_v(D) = (\text{ord}_v(\pi)/\text{ord}_v(q))[F_v : \mathbb{Q}_p] \bmod \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. The corresponding isogeny class of simple abelian varieties over κ has members with dimension $g = (1/2)[F : \mathbb{Q}] \cdot \sqrt{[D : F]}$.*

Remark 6.5. In the terminology of Theorem 4.6, the three cases in Corollary 6.4 correspond to A that is respectively of Type III with $e = 1$, Type III with $e = 2$, and Type IV.

By inspection, the formula for the dimension g in case (3) of Corollary 6.4 also works in cases (1) and (2). In particular, the common \mathbb{Q} -degree $[F : \mathbb{Q}]\sqrt{[D : F]}$ of maximal commutative subfields of D is always equal to $2g$. This shows that simple abelian varieties over finite fields always have sufficiently many complex multiplications, so by passing to products and using Theorem 4.2 we obtain:

Corollary 6.6 (Tate). *Every abelian variety A over a finite field admits sufficiently many complex multiplications. If A is isotypic then it admits a structure of CM abelian variety with complex multiplication by a CM field.*

Example 6.7. Here are some examples of simple abelian surfaces (over prime fields of any characteristic) that are not absolutely simple. Let κ be a finite field of size p^2 , with p a prime. As in Corollary 6.4(2), there is a supersingular elliptic curve E over κ whose geometric endomorphism algebra is not defined over κ (in fact, $\text{End}^0(E) = \mathbb{Q}(\sqrt{-1})$ with p^2 -Frobenius equal to $\pm p\sqrt{-1}$) and the abelian surface $A = \text{Res}_{\kappa/\mathbb{F}_p}(E)$ is a simple abelian variety over \mathbb{F}_p . But $A_\kappa \simeq E \times E'$ where E' is the twist of E by the non-trivial automorphism of κ over \mathbb{F}_p , so A_κ is not simple. Note that A_κ must be isotypic, since $E' = E^{(p)}$ is isogenous to E via the relative Frobenius morphism $E \rightarrow E^{(p)}$.

Taking K'/\mathbb{Q} to be a quadratic field in which p is inert, we can lift E over $\mathcal{O}_{K',(p)}$ to get an elliptic curve \mathcal{E} over K' having good reduction E at $p\mathcal{O}_{K'}$. Then $\mathcal{A} := \text{Res}_{K'/\mathbb{Q}}(\mathcal{E})$ is an abelian surface over \mathbb{Q} having good reduction $\text{Res}_{\kappa/\mathbb{F}_p}(E)$ at p that is simple over \mathbb{F}_p , so (via consideration of Néron models over $\mathbb{Z}_{(p)}$) \mathcal{A} is simple over \mathbb{Q} . However, $\mathcal{A}_{K'} \simeq \mathcal{E} \times \mathcal{E}'$ where \mathcal{E}' is the twist $\sigma^*(\mathcal{E})$ by the non-trivial automorphism σ of K' over \mathbb{Q} , so $\mathcal{A}_{K'}$ is not simple.

Example 6.8. Pushing the preceding example further over \mathbb{Q} , we now prove that if $p \equiv 3 \pmod{4}$ then \mathcal{E} and \mathcal{E}' are not isogenous, so $\mathcal{A}_{K'}$ is *not* isotypic (in contrast with its reduction A_κ). Suppose that there were an isogeny $\psi : \mathcal{E} \rightarrow \mathcal{E}'$, and choose it with minimal degree. In particular, ψ is not divisible by $[p]_{\mathcal{E}}$. We claim that $\text{ord}_p(\deg \psi)$ is odd (and in particular, is positive). Suppose otherwise, so $\deg \psi = mp^{2n}$ with $n \geq 0$ and $p \nmid m$. Consider the reduction $\psi_0 : E \rightarrow E^{(p)}$ of ψ , so this is an isogeny with degree mp^{2n} as well. In particular, $\ker \psi_0 \subset E$ is a finite subgroup scheme with order mp^{2n} , so its p -part has order p^{2n} . But E is supersingular, so it has a unique subgroup scheme of each p -power order. Hence, the p -part of $\ker \psi_0$ is $E[p^n]$, so $\psi_0 = \psi'_0[p^n]_E$ with $\psi'_0 : E \rightarrow E^{(p)}$ of degree m . But now consider the composite isogeny

$$E \xrightarrow{\psi'_0} E^{(p)} \xrightarrow{F} E^{(p^2)} = E$$

using the Frobenius isogeny of $E^{(p)}$. This is an endomorphism of E with degree pm . But $\text{End}(E)$ is an order in $\mathbb{Z}[i]$ on which the degree is computed as the norm to \mathbb{Z} , so we get an element of $\mathbb{Z}[i]$ whose norm in \mathbb{Z} is divisible exactly once by p . That is impossible since $p \equiv 3 \pmod{4}$, and so completes the verification that $\deg \psi$ has p -part p^j for some odd j .

We conclude that the finite K' -subgroup $N := \ker \psi \subset \mathcal{E}$ has non-trivial p -part, and this must also have cyclic geometric fiber (as otherwise it would contain $\mathcal{E}[p]$, contradicting that we arranged ψ to not be divisible by $[p]_{\mathcal{E}}$). By cyclicity, $N[p]$ is a K' -subgroup of \mathcal{E} with order p . Consider its scheme-theoretic closure G in the Néron model of \mathcal{E} at $p\mathcal{O}_{K'}$. This is a finite flat group scheme over $R = \mathcal{O}_{K',(p)}$ of order p , and its special fiber G_κ is an order- p subgroup scheme of the supersingular elliptic curve E , so $G_\kappa \simeq \alpha_p$ as κ -groups. But R is an absolutely unramified discrete valuation ring, so there are no finite flat group schemes over R with special fiber α_p [38]. This contradiction shows that \mathcal{E} and \mathcal{E}' are not isogenous (so $\mathcal{A}_{K'}$ is not isotypic), as claimed.

The proof of the surjectivity aspect of the Honda–Tate theorem requires constructing many abelian varieties over a fixed but arbitrary finite field κ . The idea is to begin with the existence part of Proposition 5.3 over $\overline{\mathbb{Q}}$, descend to a number field, use the theory of good reduction to make abelian varieties over large finite extensions of κ , and then use Weil restriction to make the required abelian varieties over the initial finite field κ . (See [22] or [51, Lemme 3] for details.) This relates simple abelian varieties over finite fields to simple factors of reductions of CM abelian varieties over number fields, at least after some finite extension on the initial finite field. But one can ask (as Honda did) whether it is possible to do better than just be a simple factor of the reduction of a CM abelian variety over a number field. As an application of the full force of the Honda–Tate theorem, Tate proved such an improved lifting theorem (which is really the starting point for the many lifting questions about CM abelian varieties that we will consider):

Theorem 6.9. *Let A be an abelian variety simple over a finite field κ . There exists a finite extension κ'/κ such that $A_{\kappa'}$ is isogenous to the reduction of a CM abelian variety with good reduction over a p -adic field with residue field κ' .*

Proof. By Corollary 6.6, there is a CM field $L \subset \text{End}^0(A)$ with $[L : \mathbb{Q}] = 2 \dim(A)$. Thus, [51, Thm. 2] may be applied to construct the required κ' and CM abelian variety over a p -adic field with residue field κ' . \blacksquare

7. A THEOREM OF GROTHENDIECK AND A CONSTRUCTION OF SERRE

Let A be an abelian variety over a field K and let $K_1 \subset K$ be a subfield. We say that A is defined over K_1 if there exists an abelian variety A_1 over K_1 and an isomorphism $\alpha : A \simeq A_{1/K}$. We use similarly terminology for a map $A \rightarrow B$ between abelian varieties over K .

For example, suppose K/K_1 is a primary extension of fields and consider abelian varieties A and B over K such that there are isomorphisms $\alpha : A \simeq A_{1/K}$ and $\beta : B \simeq B_{1/K}$ for abelian varieties A_1 and B_1 over K_1 . By Lemma 2.2, the pairs (A_1, α) and (B_1, β) are unique up to unique isomorphism and every map $A \rightarrow B$ as abelian varieties over K is defined over K_1 in the sense that it uniquely descends to a map $A_1 \rightarrow B_1$ as abelian varieties over K_1 . Likewise, by Corollary 2.4, all abelian subvarieties of A are defined over K_1 (and even arise from abelian subvarieties of A_1). For general extensions K/K_1 (with K_1 not separably closed) such K_1 -descents do not exist, and when (A_1, α) does exist it is not necessarily unique (up to isomorphism).

Example 7.1. Assume $\text{char}(K) = 0$ and let F/K is an algebraically closed extension (a basic example of interest being $F = \mathbb{C}$). We claim that each member of the isogeny class of A_F is defined over the algebraic closure \overline{K} of K in F (and hence over a finite extension of K in F). To prove this, observe that the kernel of any isogeny $\psi : A_F \rightarrow B$ over F is contained in some torsion subgroup $A[n]_F$, and $A[n]$ becomes constant over \overline{K} (since $A[n]$ is K -étale when $\text{char}(K) = 0$). Hence, we can descend $\ker \psi$ to a constant finite subgroup of $A_{\overline{K}}$, and the quotient by this gives a descent of (B, ψ) to a quotient of $A_{\overline{K}}$.

Example 7.2. When $\text{char}(K) = p > 0$, the naive analogue of Example 7.1 fails. An interesting counterexample is $A_1 = E^2$ for a supersingular elliptic curve E over an algebraically closed field K_1 of characteristic $p > 0$ (such as $\overline{\mathbb{F}}_p$). There is a canonical copy of α_p^2 in A using the unique $\alpha_p \subset E$ (the kernel of the Frobenius isogeny of E), and over a field of characteristic $p > 0$ the non-trivial proper subgroups of α_p^2 are parameterized by lines in a plane. Thus, if K/K_1 is a non-trivial extension then there are K -subgroups $G \subset A := A_{1/K}$ of order p that are contained in $\alpha_{p/K}^2$ and do not arise from a K_1 -subgroup of A_1 . In contrast with what we saw in Example 7.1 for isogeny classes over algebraically closed fields of characteristic 0, the isogenous quotient A/G of $A = A_{1/K}$ cannot be defined over K_1 as an abstract abelian variety!

Indeed, if there were an isomorphism $A/G \simeq B_{1/K}$ for an abelian variety B_1 over K_1 then the resulting isogeny

$$A_{1/K} = A \twoheadrightarrow A/G \simeq B_{1/K}$$

must descend to an isogeny $A_1 \rightarrow B_1$ over K_1 by Lemma 2.2. The kernel of this latter isogeny is a K_1 -subgroup of A_1 that descends $G \subset A$, contrary to how G was chosen. Thus, no such B_1 exists.

One lesson we learn from Example 7.1 and Example 7.2 is that the study of fields of definition for abelian varieties in positive characteristic is rather more subtle than in characteristic 0, even when working over algebraically closed base fields.

To fully appreciate the significance of Example 7.2 in positive characteristic, we now turn our attention to a striking result of Grothendieck concerning the field of definition of an abelian variety with sufficiently many complex multiplications in positive characteristic. Before stating Grothendieck's result, we should record the analogue in characteristic 0 that is the source of inspiration.

Theorem 7.3 (Shimura–Taniyama). *Every abelian variety A with sufficiently many complex multiplications over an algebraically closed field K of characteristic 0 is defined (along with its entire endomorphism algebra) over a number field in K .*

Proof. By Example 7.1, it is harmless to pass to an isogenous abelian variety. Thus, by Proposition 3.4 we can pass to the isotypic (and even simple) case, and so by Theorem 4.2 the abelian variety A over K admits complex multiplication by a CM field L . Let Φ be the resulting CM type on L .

We just have to descend the abelian variety to $\overline{\mathbb{Q}}$ since the endomorphism algebra will then automatically descend to $\overline{\mathbb{Q}}$ (by Lemma 2.2) and then by direct limit considerations we may descend to a number field. Proposition 5.3 shows that there is a CM abelian variety B over $\overline{\mathbb{Q}}$ with complex multiplication by L and CM type Φ , and B_K is L -linearly isogenous to A via comparison of CM types on L . Hence, once again using Example 7.1, we are done. ■

Theorem 7.3 can be formulated with a general ground field K of characteristic 0, but the nature of the descent becomes a bit more subtle. Namely, if A is an abelian variety over a field K of characteristic 0 and if A admits sufficiently many complex multiplications, then there is a finite extension K'/K such that $A_{K'}$ descends (along with its entire endomorphism algebra) to an abelian variety over a number field contained in K . In this formulation it is crucial to introduce the finite extension K'/K , even if we just wish to descend the abelian variety (and not any specific endomorphisms). This is illustrated by quadratic twists of elliptic curves:

Example 7.4. Consider a CM elliptic curve over \mathbb{C} and extend scalars to $K = \mathbb{C}(t)$. Let E be the quadratic twist of this scalar extension by a quadratic extension K'/K , so E is a CM elliptic curve over K whose ℓ -adic representation for $\text{Gal}(K_s/K)$ is non-trivial. No member of the isogeny class of E over K can be defined over \mathbb{C} (let alone over $\overline{\mathbb{Q}}$), as all members of the isogeny class have non-trivial action by $\text{Gal}(K_s/K)$ in their ℓ -adic representations. Of

course, if we pass up to \overline{K} then the effect of quadratic twisting goes away and there is no obstruction to descent to $\overline{\mathbb{Q}}$.

Since every abelian variety over $\overline{\mathbb{F}}_p$ descends to a finite field and hence has sufficiently many complex multiplications (by Corollary 6.6), a naive first guess for an analogue of Theorem 7.3 is that CM abelian varieties over algebraically closed fields with positive characteristic can always be descended to the algebraic closure of the prime field. Example 7.2 shows that this is false. Allowing isogenies does not eliminate the need for a finite extension:

Example 7.5. Example 7.4 easily adapts to work over $\kappa(t)$ by beginning with an elliptic curve over any finite field κ (which always has complex multiplication by an imaginary quadratic field). One can do likewise over $\overline{\mathbb{F}}_p(t)$.

Motivated by the above counterexamples in positive characteristic, Grothendieck proved a reasonable analogue of Theorem 7.3:

Theorem 7.6 (Grothendieck). *Let A be an abelian variety over a field K with $\text{char}(K) = p > 0$, and assume A admits sufficiently many complex multiplications. Then there exists a finite extension $K \subset K'$, a finite subfield $\kappa \subset K'$, and an abelian variety B over κ such that $A \otimes_K K'$ and $B \otimes_\kappa K'$ are isogenous.*

For an exposition of Grothendieck's proof, see [39]. The essential difficulty in the proof (in contrast with characteristic 0) is that the isogeny cannot be avoided, as shown by Example 7.2. The proof of Theorem 7.6 is immediately reduced to the case when K is finitely generated over the prime field \mathbb{F}_p , and Grothendieck constructed the required descent to a finite field by using the theory of potentially good reduction and to find the required K'/K and made the descent from K' via a suitable Chow trace (in the sense of [9, §6]).

There is a refinement of Grothendieck's theorem, due to Yu, that clarifies the role of the isogeny and proceeds in a simpler way by using moduli spaces of abelian varieties. To explain the refinement, we need a technique to modify the endomorphism ring. More specifically, consider an abelian variety A of dimension $g > 0$ over a field K such that A admits sufficiently many complex multiplications, and let $P \subset \text{End}^0(A)$ be a commutative semisimple \mathbb{Q} -subalgebra with $[P : \mathbb{Q}] = 2g$. Since $\text{End}(A)$ is a lattice of full rank in the \mathbb{Q} -vector space $\text{End}^0(A)$, the intersection $\mathcal{O} = P \cap \text{End}(A)$ is an order in P but it may not be the maximal order (i.e., it may not be $\mathcal{O}_P := \prod \mathcal{O}_{L_i}$ where $\prod L_i$ is the decomposition of P into a finite product of number fields). It is natural to ask if we can pass to an isogenous abelian variety for which this problem goes away,

Example 7.7. Consider the preceding setup with $K = \mathbb{C}$. In this case we have an analytic uniformization $A^{\text{an}} = V/\Lambda$ in which V is a \mathbb{C} -vector space equipped with a \mathbb{C} -linear action by P and Λ is a lattice stable under the order \mathcal{O} . Then $\Lambda' = \mathcal{O}_P \cdot \Lambda$ is an \mathcal{O}_P -stable lattice in V and V/Λ' is an isogenous quotient of A^{an} on which \mathcal{O}_P naturally acts. This algebraizes to an isogenous quotient A' of A such that under the identification $\text{End}^0(A') = \text{End}^0(A)$ we have $P \cap \text{End}(A') = \mathcal{O}_P$.

We seek an algebraic variant of the analytic construction in Example 7.7. Observe that $\mathcal{O}_P \cdot \Lambda$ is the image of the natural map $\mathcal{O}_P \otimes_{\mathcal{O}} \Lambda \rightarrow V$. Inspired by this, we are led to ask if

these is a way to enlarge an endomorphism ring via a “tensor product” against a finite-index extension of coefficient rings. There is a construction of this sort due to Serre [44], applicable over any base scheme, though it turns out to not be applicable to the above situation because \mathcal{O}_P is not a projective \mathcal{O} -module when $\mathcal{O} \neq \mathcal{O}_P$. We wish to adapt Serre’s construction to the above situation over a field, so we first explain Serre’s procedure.

Consider a scheme S , a commutative ring \mathcal{O} , and an \mathcal{O} -module scheme A over S . Using that M is projective, one shows that the functor $T \rightsquigarrow M \otimes_{\mathcal{O}} A(T)$ on S -schemes is represented by an S -scheme, denoted $M \otimes_{\mathcal{O}} A$, and that $M \otimes_{\mathcal{O}} A$ inherits many nice properties from A : preservation of flatness, smoothness, properness; good behavior with respect to analytification over \mathbb{C} ; etc. (The interested reader can see [10, §7] for more details, where non-commutative \mathcal{O} are also considered.)

The idea of the construction of $M \otimes_{\mathcal{O}} A$ is that if $\mathcal{O}^r \xrightarrow{\varphi} \mathcal{O}^s \rightarrow M \rightarrow 0$ is a presentation then we want to take $M \otimes_{\mathcal{O}} A$ to be the cokernel of the S -group map $A^r \rightarrow A^s$ induced by the matrix of φ . Over a general base scheme S such a quotient may not exist. However, since M is projective we can instead begin with a presentation of the dual module M^* and then dualize to get a left-exact sequence $0 \rightarrow M \rightarrow \mathcal{O}^s \rightarrow \mathcal{O}^r$ and construct $M \otimes_{\mathcal{O}} A$ as a scheme-theoretic kernel.

When working over a field the cokernel idea is less problematic, so we can avoid dualizing M and hence the method works with weaker hypotheses on M . Here is a version for abelian varieties.

Proposition 7.8. *Let A be an abelian variety over a field K . Let $\mathcal{O} \subset \text{End}(A)$ be a commutative subring. For any finitely generated \mathcal{O} -module M , the functor $T \rightsquigarrow M \otimes_{\mathcal{O}} A(T)$ on K -schemes has fppf sheafification that is represented by an abelian variety $M \otimes_{\mathcal{O}} A$.*

For a map $M \rightarrow N$ between torsion-free \mathcal{O} -modules with finite cokernel, the induced map $M \otimes_{\mathcal{O}} A \rightarrow N \otimes_{\mathcal{O}} A$ is an isogeny. In particular, if \mathcal{O}' is a torsion-free \mathcal{O} -algebra that is finitely generated as an \mathcal{O} -module then the natural map of abelian varieties $A \rightarrow A' := \mathcal{O}' \otimes_{\mathcal{O}} A$ is an isogeny and the identification $\text{End}^0(A) = \text{End}^0(A')$ carries $\mathcal{O}' \subset \text{End}^0(A)$ into $\text{End}(A')$.

Beware that the notation $\mathcal{O}' \otimes_{\mathcal{O}} A$ should not be confused with the standard notation for affine base change of schemes (i.e., $X \otimes_R R'$ as shorthand for $X \times_{\text{Spec } R} \text{Spec } R'$). The context should always make the meaning clear, and we will only rarely use the Serre construction or its variants anyway.

Proof. Choose a finite presentation of \mathcal{O} -modules

$$\mathcal{O}^r \xrightarrow{\varphi} \mathcal{O}^s \longrightarrow M \rightarrow 0.$$

The map φ is given by an $s \times r$ matrix over \mathcal{O} , and so it defines an analogous map $[\varphi] : A^r \rightarrow A^s$ between abelian varieties over K . Define the abelian variety quotient $M \otimes_{\mathcal{O}} A = \text{coker}([\varphi]) := A^s / [\varphi](A^r)$. Since we are working over a field, the map $[\varphi]$ is faithfully flat onto its image abelian variety in A^s . Hence, $M \otimes_{\mathcal{O}} A$ represents the cokernel of $[\varphi]$ as fppf abelian sheaves over K . It follows (via the right-exactness of algebraic tensor products) that the abelian variety $M \otimes_{\mathcal{O}} A$ represents the fppf sheafification of $T \rightsquigarrow M \otimes_{\mathcal{O}} A(T)$.

Let $M \rightarrow N$ be a map between torsion-free \mathcal{O} -modules with finite cokernel. There is a map $N \rightarrow M$ such that both composites $M \rightarrow M$ and $N \rightarrow N$ are multiplication by a common non-zero integer n . Hence, we get maps in both directions between $M \otimes_{\mathcal{O}} A$ and $N \otimes_{\mathcal{O}} A$ whose composites are each equal to multiplication by n , so both maps between $M \otimes_{\mathcal{O}} A$ and $N \otimes_{\mathcal{O}} A$ are isogenies.

The assertions concerning \mathcal{O}' follow by considering the functor represented by $\mathcal{O}' \otimes_{\mathcal{O}} A$. \blacksquare

Remark 7.9. When the base is not a field, the projectivity hypothesis on M over \mathcal{O} in Serre's construction is necessary. In fact, there is an affine integral scheme S , abelian scheme $A \rightarrow S$, and commutative field $L \subset \text{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(A)$ such that there is no isogeny $A \rightarrow A'$ to another abelian scheme over S with the equality $\text{End}^0(A) = \text{End}^0(A')$ carrying \mathcal{O}_L into $\text{End}(A')$. In particular, there is no analogue of Proposition 7.8 over such a base S . (Note that in any such situation some order of \mathcal{O}_L lies in $\text{End}(A')$ and $\text{End}(A)$, as both endomorphism rings are \mathbb{Z} -lattices of full rank in the \mathbb{Q} -algebra $\text{End}^0(A) = \text{End}^0(A')$.)

For example, let $S = \text{Spec } R$ where R is the index p -order $\mathbb{Z}_{(p)} + p \cdot \mathbb{Z}_{(p)}[i]$ in $\mathbb{Z}_{(p)}[i]$ with a prime $p \equiv 3 \pmod{4}$ and $i^2 = -1$, and let E be the elliptic curve $y^2 = x^3 - x$ viewed over S . The generic fiber has endomorphism ring $\mathbb{Z}[i]$, with i acting via $[i](x, y) = (-x, -iy)$, so $[i]^*(dy/x) = i \cdot dy/x$. Hence, $[i]$ acts as multiplication by $i \in \mathbb{Q}(i) = \text{Frac}(R)$ on the tangent space, and this property is inherited by the generic fiber of any elliptic curve E' over R equipped with an isogeny from E (using the resulting identification $\text{End}^0(E'_{\mathbb{Q}(i)}) = \text{End}^0(E_{\mathbb{Q}(i)})$ to transfer the $\mathbb{Z}[i]$ -action over to $E'_{\mathbb{Q}(i)}$). But $i \notin R$, so no such E' can admit an action by $\mathbb{Z}[i]$ over R respecting the action on its generic fiber.

Now we can give Yu's refinement of Theorem 7.6, which asserts that we can *first* apply an isogeny and *then* pass to a finite extension on K (with no further isogeny involved) to get to a situation that descends to a finite field. Consider the setup in Theorem 7.6. By Proposition 3.4, the simple factors all have sufficiently many complex multiplications, so we may and do focus on the case of simple abelian varieties A . Choose a polarization, so $D = \text{End}^0(A)$ is endowed with a positive involution. By [55, 2.2], there is a maximal commutative subfield $L \subset D$ that is stable under the involution, so L is either totally real or CM. We claim that L must be a CM field, or in other words L is not totally real.

To prove this property of L , first note that by Proposition 4.7 (in positive characteristic) the division algebra D is either of Type III or Type IV (in the sense of Theorem 4.6). Since L contains the center F of D , for Type IV we get the CM property for L from the fact that F is CM in such cases. For Type III, the key point is that F is totally real and D is non-split at all real places of F . We know that D_L is split over L since L is a maximal commutative subfield of D , so L cannot be totally real. Hence, once again L must be a CM field.

Applying Proposition 7.8, we can pass to an isogenous abelian variety to arrange that $\mathcal{O}_L \subset \text{End}(A)$. In this special case, it turns out that for some finite extension K'/K we can descend $A_{K'}$ with its \mathcal{O}_L -action to a finite field. Note that it actually suffices to just descend the abelian variety $A_{K'}$ to a finite field, as then a further finite extension on K' will enable us to descend the abelian variety along with its \mathcal{O}_L -action, by Lemma 2.2.

Theorem 7.10 (Yu). *Let K be a field with positive characteristic, and A an isotypic CM abelian variety over K with CM structure provided by a CM field $L \subset \text{End}^0(A)$. If $\mathcal{O}_L \subset \text{End}(A)$ then there is a finite extension K'/K such that $A_{K'}$ equipped with its \mathcal{O}_L -action descends to a finite field contained in K' .*

This result is [55, Thm. 1.3]; it will not be used in what follows.

8. CM LIFTING QUESTIONS

Now we fix a field k of characteristic $p > 0$, and we consider an abelian variety A_0 over k . By Corollary 6.6, if k is finite and A_0 is isotypic then we may endow it with a structure of CM abelian variety having complex multiplication by a CM field. Inspired in part by Theorem 6.9, we wish to pose several questions related to the problem of lifting A_0 to characteristic 0 in the presence of CM structures. First we make a general definition unrelated to complex multiplication.

Definition 8.1. *A lifting of A_0 to characteristic 0 is a triple (R, A, ϕ) consisting of a domain R of characteristic 0, an abelian scheme A over R , and an isomorphism $\phi : A \otimes_R k \simeq A_0$ of abelian varieties over k , where we use specialization of A along a surjective map $R \rightarrow k$.*

We will generally let $M = \text{Frac}(R)$, so A_M denotes the generic fiber of such an abelian scheme A over R . If A_M admits sufficiently many complex multiplications, then we say that A is a *CM lift* of A_0 to characteristic 0. The natural map $\text{End}(A) \rightarrow \text{End}(A_M)$ is always injective. The cokernel of this map is always torsion-free, due to:

Lemma 8.2. *Let A and B be abelian schemes over an integral scheme S with generic point η . The natural injective map $\text{Hom}(A, B) \rightarrow \text{Hom}(A_\eta, B_\eta)$ has torsion-free cokernel.*

Proof. Consider $f : A_\eta \rightarrow B_\eta$ such that $n \cdot f$ extends to an S -group map $h : A \rightarrow B$ for a non-zero integer n . The restriction $h : A[n] \rightarrow B[n]$ between finite flat S -groups vanishes because such vanishing holds on the generic fiber over the integral S . Since $[n] : A \rightarrow A$ is an fppf covering with kernel $A[n]$, it follows that h factors through this map over S , which is to say $h = n \cdot \tilde{f}$ for some S -group map $\tilde{f} : A \rightarrow B$. Hence, $\tilde{f}_\eta - f \in \text{Hom}(A_\eta, B_\eta)$ is killed by n , so $\tilde{f}_\eta = f$. ■

The injective map in Lemma 8.2 can fail to be surjective:

Example 8.3. Let p be a prime with $p \equiv 3 \pmod{4}$, so p is prime in $\mathbb{Z}[i]$ (with $i^2 = -1$). Let R be the order $\mathbb{Z}_{(p)} + p\mathbb{Z}_{(p)}[i]$ of index p in $\mathbb{Z}_{(p)}[i]$, so $\text{Frac}(R) = \mathbb{Q}(i)$. Let E be the elliptic curve $y^2 = x^3 - x$ viewed over R , so the generic fiber $E_{\mathbb{Q}(i)}$ has endomorphism ring $\mathbb{Z}[i]$ via the action $[i](x, y) = (-x, iy)$. As we saw in Remark 7.9, $\mathbb{Z}[i]$ acts on $T_0(E_{\mathbb{Q}(i)})$ through scaling via the canonical inclusion $\mathbb{Z}[i] \hookrightarrow \mathbb{Q}(i)$.

We claim that $\text{End}(E) = \mathbb{Z}$ (so $\text{End}^0(E) := \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(E) = \mathbb{Q}\mathbb{Q}$, even though the generic fiber $E_{\mathbb{Q}(i)}$ has endomorphism algebra $\mathbb{Q}(i)$). Indeed, if not then $\text{End}(E)$ is an order in $\mathbb{Z}[i] = \text{End}(E_{\mathbb{Q}(i)})$, so by Lemma 8.2 we would have $\text{End}(E) = \mathbb{Z}[i]$. In particular, the action

by i on $E_{\mathbb{Q}(i)}$ would extend to an action on E , and so the resulting multiplier action by i on the tangent line $T_0(E_{\mathbb{Q}(i)}) = T_0(E) \otimes_R \mathbb{Q}(i)$ would preserve the R -submodule $T_0(E)$. But $T_0(E)$ is a free R -module of rank 1 since R is local and E is R -smooth, so the i -action on this R -module would have to be multiplication by some element $r \in R$. But working over $\mathbb{Q}(i)$ we have seen that we get the multiplier i , so necessarily $r = i$. But $i \notin R$ due to the definition of R , so we have a contradiction.

In the preceding example, the base ring R is not normal. This is essential, since in the normal case there is no obstruction to extending maps between abelian schemes:

Lemma 8.4. *For a normal domain R with fraction field M , the functor $A \rightsquigarrow A_M$ from abelian schemes over R to abelian varieties over M is fully faithful.*

Proof. This is a special case of a general lemma of Faltings [16, §2, Lemma 1]. ■

For normal R we get a specialization map

$$\mathrm{End}^0(A_M) = \mathrm{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(A) \rightarrow \mathrm{End}^0(A_\kappa) = \mathrm{End}^0(A_0)$$

for endomorphism algebras, and likewise for endomorphism rings. This makes normality a natural property to impose on R when studying questions about CM lifts. In general, if R is not normal then we cannot directly compare the endomorphism algebras on the generic fiber and the κ -fiber, so we just have the specialization map of endomorphism algebras $\mathrm{End}^0(A) \rightarrow \mathrm{End}^0(A_\kappa)$. This map can fail to be surjective. An elementary example is an elliptic curve over $\mathbb{Z}_{(p)}$ for a prime p (since elliptic curves over finite fields always admit complex multiplication, whereas elliptic curves over \mathbb{Q} always have endomorphism algebra \mathbb{Q}). The specialization map of endomorphism rings $\mathrm{End}(A) \rightarrow \mathrm{End}(A_\kappa)$ can also have cokernel that is not torsion-free, even when R is normal. (We will see natural examples of this phenomenon in our study of CM lifting problems, when we consider lifting questions for specific orders in CM fields.)

Now we turn to the lifting questions that we shall study. Fix a finite field \mathbb{F}_q of size q , and an abelian variety B of dimension $g > 0$ over \mathbb{F}_q . Assume that B is isotypic over \mathbb{F}_q (which is necessary and sufficient in order that B admit a structure of CM abelian variety with complex multiplication by a CM field, by Theorem 3.1 and Corollary 6.6). Let B_κ denote the scalar extension of B over a finite extension field κ/\mathbb{F}_q . Consider the following five assertions concerning the existence of a CM-lifting of B or B_κ .

- (CML) *CM lifting*: there exists a local domain R with characteristic 0 and residue field \mathbb{F}_q , an abelian scheme A over R with relative dimension g equipped with a CM field $L \subset \mathrm{End}^0(A)$ satisfying $[L : \mathbb{Q}] = 2g$, and an isomorphism $\phi : A \otimes_R \mathbb{F}_q \simeq B$ as abelian varieties over \mathbb{F}_q .
- (R) *CM lifting after finite residue field extension*: there exists a local domain R with characteristic 0 and residue field κ of finite degree over \mathbb{F}_q , an abelian scheme A over R with relative dimension g equipped with an action (in the isogeny category over R) by a CM field L with $[L : \mathbb{Q}] = 2g$, and an isomorphism $\phi : A \otimes_R \kappa \simeq B_\kappa$ as abelian varieties over κ .

- (I) *CM lifting up to isogeny*: there exists a local domain R with characteristic 0 and residue field \mathbb{F}_q , an abelian scheme A over R with relative dimension g equipped with an action (in the isogeny category over R) by a CM field L with $[L : \mathbb{Q}] = 2g$, and an isogeny $A \otimes_R \mathbb{F}_q \rightarrow B$ of abelian varieties over \mathbb{F}_q .
- (NI) *CM lifting to normal domains up to isogeny*: there exists a normal local domain R with characteristic 0 and residue field \mathbb{F}_q such that (I) is satisfied for B using R .
- (NIR) *CM lifting to normal domains up to isogeny after finite residue field extension*: there exists a normal local domain R with characteristic 0 and residue field κ of finite degree over \mathbb{F}_q such that (R) is satisfied for B using R except that ϕ is only required to be an isogeny over κ rather than an isomorphism.

Remark 8.5. By expressing a local ring as a direct limit of local subrings essentially of finite type over \mathbb{Z} , it follows that in the formulation of (R) there is no loss of generality in replacing κ with an algebraic closure of \mathbb{F}_q or allowing κ to vary over all extensions of \mathbb{F}_q .

Observe that by Theorem 6.9, (NIR) always has an affirmative answer for any isotypic B over \mathbb{F}_q , and the CM lift can be chosen using any CM maximal commutative subfield $L \subset \text{End}^0(B)$. There are several questions we wish to answer in the direction of refining this fact:

- (1) Is a residue field extension necessary? That is, does (NI) always hold?
- (2) If (NI) does not always hold, can we characterize when it holds? And how about (I) in general (i.e., drop normality, but permit an isogeny without increasing the residue field)?
- (3) Is an isogeny necessary? That is, does (R) always hold, or perhaps even (CML)?

These questions can be made more specific in several respects. For example, since the simple $\text{End}^0(B)$ is generally non-commutative, it generally contains more than one CM maximal commutative subfield L (up to conjugacy) and so we can pose the CM lifting questions requiring an order in a particular choice of L to lift to a CM structure over R . We will give examples to show that the choice of such an L can affect the nature of the answer to some of the lifting questions. But even if we know that for a given B and choice of $L \subset \text{End}^0(B)$ it is possible to construct a CM lift to characteristic 0 on which the action of an order in L also lifts, it could be that the full CM order $L \cap \text{End}(B)$ does not lift. We will give examples where this happens.

Here are answers to the above questions. The proofs form the backbone of the present volume.

- As we will describe in §9, there exist abelian varieties over $\overline{\mathbb{F}}_p$ which do not admit a CM lift to characteristic 0. Thus, (R) does not hold in general, so in particular (CML) does not always hold. Hence, *an isogeny is necessary*; that is, it is better to consider (I) than (CML).
- We will prove that (I) always holds. In fact, for any CM maximal commutative subfield $L \subset \text{End}^0(B)$ we will construct an isogeny $B \rightarrow A_0$ to an abelian variety over \mathbb{F}_q such that A_0 has a CM lift to characteristic 0 on which the action of the order $\mathbb{Z} + p\mathcal{O}_L$ in \mathcal{O}_L also lifts. However, A_0 will generally depend on L .

- In contrast with the success with (I), if we want to impose a normality requirement on R and not increase the residue field (but permit isogenies) then the answer is negative. That is, we will give examples for which (NI) fails. Hence, the existence of a CM lifting to a normal domain of characteristic 0 must generally allow a finite extension of the initial finite field (and an isogeny), exactly as in Theorem 6.9. However, we there is a good salvage: for each B and choice of $L \subset \text{End}^0(B)$ we will give concrete *necessary and sufficient* conditions in terms of CM types on L for (NI) to have an affirmative answer with a CM lifting to which the action of an order in L also lifts. We will also give examples of B for which this necessary and sufficient condition is satisfied for one choice of $L \subset \text{End}^0(B)$ but fails for another choice. ¹

9. AN ISOGENY IS NECESSARY.

In this section we review some results from [42], especially concerning the failure of (R). In view of Remark 8.5, to give a counterexample to (R) in characteristic p it suffices to give a simple abelian variety over $\overline{\mathbb{F}}_p$ not admitting a CM lifting to characteristic 0. Note that since $\overline{\mathbb{F}}_p$ is algebraically closed, there is no loss of generality in restricting attention to CM lifts over complete discrete valuation rings of characteristic 0, so the generic fiber of such a lifting must be simple too.

To motivate the examples over $\overline{\mathbb{F}}_p$, it is instructive to first begin with an example involving a ground field of positive transcendence degree over \mathbb{F}_p . Consider an abelian variety B over a field K with characteristic $p > 0$ such that B admits sufficiently many complex multiplications but B cannot be defined over a finite subfield of K . In Example 7.2 we saw such B that are abelian surfaces.

Proposition 9.1. *For every extension of fields K'/K , the abelian variety $A_0 := B_{K'}$ does not admit a lifting to characteristic 0 with sufficiently many complex multiplications on its generic fiber.* ²

That is, there is no abelian scheme A over a local domain R with characteristic 0 and residue field K' containing K such that the generic fiber A_M over $M = \text{Frac}(R)$ admits sufficiently many complex multiplications and the special fiber $A_{K'}$ is isomorphic to A_0 .

Proof. We first check that the choice of K'/K does not actually matter: if K'/K is an extension of field with characteristic $p > 0$ and if B is an abelian variety over K such that $B' := B_{K'}$ is defined over a finite subfield of K' then we claim that B is defined over a finite subfield of K .

To prove this, let $k \subset K$ and $k' \subset K'$ be the respective algebraic closures of \mathbb{F}_p , so it is harmless ³ to replace K' with the subfield $k'K = k' \otimes_k K$ inside of K' . By direct

¹Likely such example: $B = E \times E$ over \mathbb{F}_{p^2} with $\pi_E = -p$. All geometric endomorphisms defined over \mathbb{F}_{p^2} . Take CM field L_1 with p totally ramified; (NI) satisfied. Take CM field L_2 Galois over \mathbb{Q} with p totally inert; (NI) fails.

²Example 7.5 gives counterexamples.

³This is the error. Example 7.5 gives counterexamples.

limit considerations we may also then shrink k' so that $[k' : k]$ is finite. By hypothesis, B' descends to an abelian variety B'_0 over k' . By direct limit arguments with finite subfields of k , it suffices to descend B to k . The finite Galois group $\text{Gal}(k'/k) = \text{Gal}(K'/K)$ naturally acts on $B' = B_{K'}$ over its action on $K' = k' \otimes_k K$. But $B' = B'_0 \otimes_{k'} K'$, and the extension K'/k' is primary in the sense of field theory (i.e., k' is separably closed in K'). Thus, by Lemma 2.2, the Galois action on B' over K' descends to one on B'_0 over k' . This latter action descends B'_0 to an abelian variety B_0 over k , and it is easy to check that the resulting isomorphism

$$(B_0 \otimes_k K) \otimes_K K' \simeq (B_0 \otimes_k k') \otimes_{k'} K' \simeq B'_0 \otimes_{k'} K' \simeq B' = B \otimes_K K'$$

is $\text{Gal}(K'/K)$ -equivariant. Hence, it descends to a K -isomorphism $B_0 \otimes_k K \simeq B$ which expresses B_0 as a descent of B to the subfield $k \subset K$, as required.

Returning to our initial setup, suppose to the contrary that for some extension K'/K there exists a lifting A of $B_{K'}$ to characteristic 0 with sufficiently many complex multiplications on its generic fiber. Since the generic fiber A_M is an abelian variety with sufficiently many complex multiplications over a field M of characteristic 0, by replacing M with a finite extension and R with a localization of its normalization in M we may arrange by Theorem 7.3 that A_M descends to an abelian variety X with sufficiently many complex multiplications over a number field $M_1 \subset M$.

There is a finite extension M'_1/M_1 such that $X_{M'_1}$ acquires good reduction at all primes of M'_1 . Thus, if we increase M some more to contain M'_1 then we may arrange that R is normal and that X has good reduction at all primes of M_1 . By normality, $\mathcal{O}_{M_1} \subset R$. The maximal ideal of R has positive characteristic, so it contracts to a maximal ideal \mathfrak{p} of \mathcal{O}_{M_1} and the finite field $\kappa(\mathfrak{p})$ is naturally contained in the residue field K' of R .

Let \mathfrak{X} denote the Néron model of X over $\mathcal{O}_{M,\mathfrak{p}}$, so A and $\mathfrak{X} \otimes_{\mathcal{O}_{M_1,\mathfrak{p}}} R$ are abelian schemes over R with the same generic fiber over M . By the normality of R , this identification over M uniquely extends to one over R (Lemma 8.4). This isomorphism of abelian schemes over R induces an isomorphism $A_0 \simeq \mathfrak{X}_{\kappa(\mathfrak{p})} \otimes_{\kappa(\mathfrak{p})} K'$ between special fibers over K' . In particular, $A_0 = B_{K'}$ is defined over the finite field $\kappa(\mathfrak{p}) \subset K'$. But we have seen that no such descent to a finite field exists after any extension on K , so we have reached a contradiction. ■

In a sense, the above simple example is the leading principle for the proof of:

Theorem 9.2. *Let p be a prime number, and g and f be integers with $g \geq 3$ and $0 \leq f < g - 1$. There exists an absolutely simple g -dimensional abelian variety B over a finite field such that B does not satisfy (CML) and p -rank $f(B)$ (i.e., the height of the étale part of $B[p^\infty]$) is f .*

This result is [42, Thm. B]. Before we sketch the proof, we introduce one piece of notation: the a -number of an abelian variety A over a field K with characteristic $p > 0$ is

$$a(G) = \dim_{K'} \text{Hom}(\alpha_p, A_{K'})$$

for any perfect field K'/K (the choice of which does not matter). Here, the K' -action is through $\alpha_p \subset \mathbb{G}_a$ over K' . Concretely, $p^{a(G)}$ is the order of the maximal subgroup scheme of $A_{\overline{K}}$ whose Frobenius and Verschiebung operators vanish.

A useful principle to keep in mind is that an obstruction to (CML) is the size of the fields of definition. In the examples that we will construct, “size” should be interpreted in terms of the degree over the prime field (as a supernatural number): one uses a pro- p extension of a specific finite field in order to get an upper bound on the field of definition if (CML) is to hold. In Chapter 3 we will make an improvement on this by providing an effectively computable finite field which is an upper bound for the field of definition of the p -divisible group if (CML) is to hold. We will also show that if A is an abelian variety of dimension $g > 1$ over a finite field κ and A has p -rank at most $g - 2$ then for some finite extension κ'/κ there is a member of the isogeny class of $A_{\kappa'}$ for which (CML) fails. In this sense, the failure of (R) is ubiquitous.

Now taking up the sketch of the proof, for g and f as given one first constructs an abelian variety C over $\mathbb{F} = \overline{\mathbb{F}}_p$ such that $\text{End}^0(C)$ is a commutative field, $\dim(C) = g$, and $f(C) = f$. This rests on [28]. Then an abelian variety A over a finite subfield $\kappa \subset \mathbb{F}$ is found so that $A \otimes_{\kappa} \mathbb{F} \simeq C$, $a(A) = 2$, and there exists a quotient A/α_p with $a(A/\alpha_p) = 1$. Choosing an identification of α_p^2 with the maximal subgroup scheme of A with vanishing Frobenius and Verschiebung operators, one shows that the set of group scheme immersions $j : \alpha_p \hookrightarrow A_{\mathbb{F}} = C$ is identified with $\mathbb{P}^1(\mathbb{F})$.

Consider the various quotients $C/j(\alpha_p)$. One shows (this is the central part of the proof) that there exists a field Λ which is a pro- p -extension of a finite extension of K such that if $C/j(\alpha_p)$ satisfies (CML) then $j \in \mathbb{P}^1(\Lambda)$. Hence, for any finite subfield $\mathbb{F}_q \subset \mathbb{F}$ containing κ but not contained in Λ there exists $B = A_{\mathbb{F}_q}/j(\alpha_p)$ such that B does not satisfy (CML).

It is not so easy to give concrete examples using this proof. One can also ask if it is really necessary to find a field outside the large extension $\Lambda \supset \mathbb{F}_p$. In Chapter 3 we will come back to this question and give effective bounds which reprove the theorem, and which help in finding explicit examples of abelian varieties over a finite field not satisfying (CML).

REFERENCES

- [1] Artin, E. & Tate, J. Class field theory. Advanced Book Classics, Addison-Wesley, New York, 1990.
- [2] Berthelot, P. & Breen, L. & Messing, W. Théorie de Dieudonné cristalline II. LNM 930, Springer-Verlag 1982.
- [3] Berthelot, P. & Ogus, A. F -isocrystals and de Rham cohomology I. *Inv. Math.* 72, 1983, 159–199.
- [4] Bosch, S. & Güntzer, U. & Remmert, R. Non-archimedean analysis. Grundle. 261, Springer-Verlag, New York, 1983.
- [5] Bosch, S. & Lütkebohmert, W. & Raynaud, M. Néron models. *Ergebnisse der Mathematik* 21, Springer-Verlag, New York, 1990.
- [6] Breuil, C. Groupes p -divisibles, groupes finis et modules filtrés *Ann. of Math.* **152** (2000), 489–549.
- [7] Chai, C.-L. & Oort, F., Hypersymmetric abelian varieties, *Quarterly J. Pure Applied Math.* **2** (Coates Special Issue) (2006), 1–27.
- [8] Colmez, P. & Fontaine, J.-M. Construction des représentations p -adiques semi-stables. *Invent. Math.* 140 (2000), 1–43.

- [9] Conrad, B. Chow’s K/k -image and K/k -trace, and the Lang-Néron theorem. *Enseign. Math* (2) 52, no. 1–2 (2006), 37–108.
- [10] Conrad, B. Gross-Zagier revisited. In *Heegner points and Rankin L-series*, MSRI Publ. 49, Cambridge Univ. Press, Cambridge, 2004.
- [11] Conrad, B. Main Theorem of Complex Multiplication. In “Notes on complex multiplication”, available at www.math.stanford.edu/~conrad/.
- [12] Deligne, P. Application de la formule des traces aux sommes trigonométriques. In *Cohomologie Etale*, Séminaire de Géométrie Algébrique du Bois-Marie SGA4 $\frac{1}{2}$, LNM 569, Springer-Verlag 1977, 168–232.
- [13] Deligne, P. Motifs et groupes de Taniyama. In *Hodge Cycles, Motives, and Shimura Varieties*, LNM 900, Springer-Verlag, 1982, 261–279.
- [14] Dieudonné, J. & Grothendieck, A. Éléments de géométrie algébrique. Publ. Math. IHES 11, 1961.
- [15] Eisenträger, K. The Theorem of Honda and Tate. In “Notes on complex multiplication”, available at www.math.stanford.edu/~conrad/.
- [16] Faltings, G. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry* (Cornell/Silverman, ed.), Springer-Verlag, New York, 1986.
- [17] Fontaine, J-M. Module galoisiens, modules filtrés et anneaux de Barsotti-Tate. *Astérisque* 65, 1979, 3–80.
- [18] Fontaine, J-M. Sur certains types de représentations p -adiques du groupe de Galois d’un corps local; construction d’un anneau de Barsotti-Tate. *Annals of Math.* 115, 1982, 529–577.
- [19] Fontaine, J-M. Représentations p -adiques semi-stables. *Astérisque* 223, 1994, 113–184.
- [20] van der Geer, G. & Moonen, B. Abelian varieties. In preparation.
- [21] Hazewinkel, M. Formal groups and applications. Academic Press, New York, 1978.
- [22] Honda, T. Isogeny classes of abelian varieties over finite fields. *Journ. Math. Soc. Japan* 20 (1968), 83 – 95.
- [23] Jacobson, N. Basic algebra II. W.H. Freeman & Co., 1989.
- [24] de Jong, A.J. Crystalline Dieudonné module theory via formal and rigid geometry. *Publ. Math. IHES* 82, 1995, 5–96.
- [25] Katz, N.M. Serre-Tate local moduli. *Springer LNM* 868, 1981, 138–202.
- [26] Kisin, M. Crystalline representations and F -crystals. In *Algebraic Geometry and Number Theory*, 459–496, *Progr. Math.*, 253, Birkhser Boston, Boston, MA, 2006.
- [27] Lang, S. *Complex Multiplication*. Grundlehren mathematischen Wissenschaften 255, Springer-Verlag, 1983.
- [28] H. W. Lenstra jr, H.W & Oort, F. Simple abelian varieties having a prescribed formal isogeny type. *Journ. Pure Appl. Algebra* 4 (1974), 47 - 53.
- [29] Mazur, B. & Messing, W. Universal extensions and one-dimensional crystalline cohomology. *Springer LNM* 370, Springer-Verlag, 1974.
- [30] Messing, W. The crystals associated to Barsotti-Tate groups: with applications to abelian schemes. *Springer LNM* 264, Springer-Verlag, 1972.
- [31] Milne, J. Canonical models of (mixed) Shimura varieties and automorphic vector bundles. In *Automorphic Forms, Shimura Varieties, and L-functions*, vol. I, *Perspectives in Math.* v. 10, Academic Press, 1990, 283–414.
- [32] Milne, J. & Shih, K.-Y. Langlands’ construction of the Taniyama group. In *Hodge Cycles, Motives, and Shimura Varieties*, LNM 900, Springer-Verlag, 1982, 229–260.
- [33] Milne, J. & Waterhouse, W. Abelian varieties over finite fields. In *1969 Number Theory Institute (Prof. Sympos. Pure Math., Vol. XX, SUNY Stony Brook, NY, 1969)*, AMS, Providence, 1971, 53–64.
- [34] Milne, J. Abelian varieties. In *Arithmetic geometry* (Cornell/Silverman, ed.), Springer-Verlag, New York, 1986.
- [35] Moret-Bailly, L. *Pinceaux de variétés abéliennes*, *Astérisque* 129, 1985.
- [36] Mumford, D. *Abelian varieties*. TIFR studies in mathematics, 2008.
- [37] Norman, P. & Oort, F. Moduli of abelian varieties. *Annals of Math.*, 112 (1980), pp. 413–439.
- [38] Oort, F. & Tate, J. Group schemes of prime order *Ann. Sci. ENS* 3 (1970), pp. 1–21.

- [39] Oort, F. The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field *Journ. Pure Appl. Algebra* **3** (1973), 399–408.
- [40] Oort, F. Isogenies of formal groups. *Indag. Math.*, **37** (1975) 391–400.
- [41] Oort, F. Endomorphism algebras of abelian varieties. *Algebraic Geometry and Commut. Algebra in honor of M. Nagata* (Ed. H. Hijikata et al), Kinokuniya Cy Tokyo, Japan, 1988, Vol. II; pp. 469–502.
- [42] Oort, F. CM-lifting of abelian varieties. *J. Alg. Geom.* 1, 1992, 131–146.
- [43] Oort, F. Abelian varieties over finite fields. Summer School on "Varieties over finite fields", Göttingen, 25-VI — 6-VII-2007. Higher-dimensional geometry over finite fields. Proceedings of the NATO Advanced Study Institute 2007 (Editors: Dmitry Kaledin Yuri Tschinkel). IOS Press, 2008, pp. 123 – 188.
- [44] Serre, J-P. Complex multiplication. In *Algebraic Number Theory* (Cassels-Fröhlich, ed.), Academic Press, New York, 1967.
- [45] Serre, J-P. *Abelian ℓ -Adic Representations and Elliptic Curves*. W. A. Benjamin, 1968.
- [46] Serre, J-P. Groupes algébriques associés aux modules de Hodge-Tate. *Astérisque* **65**, 1979, 155–188.
- [47] Serre, J-P. & Tate, J. Good reduction of abelian varieties. *Ann. Math.* 88, 1965, 492–517.
- [48] Shimura, G. & Taniyama, Y. *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*. Publ. Math. Soc. Japan, 6, 1961.
- [49] Tate, J. Endomorphisms of abelian varieties over finite fields. *Inv. Math.* 2, 1966, 134–144.
- [50] Tate, J. p -divisible groups. In *Proc. Conf. on Local Fields*, Springer-Verlag, 1967, 148–183.
- [51] Tate, J. Class d'isogenie des variétés abéliennes sur un corps fini (d'après T. Honda), *Séminaire Bourbaki*, 1968/69, no. 352. LNM 179, Springer-Verlag, 1971, 95–110.
- [52] Weil, A. On a certain type of character of the idèle-class group of an algebraic number field. In *Proc. Intern. Symp. on Algebraic Number Theory*, Tokyo-Nikko, 1955, 1–7.
- [53] Yu, C.-F. Lifting abelian varieties with additional structure. *Math. Z.* **242**, 2002, 427–441.
- [54] Yu, C.-F. On reduction of Hilbert-Blumenthal varieties. *Annales de l'Institut Fourier* (Grenoble) **53**, 2003, 2105–2154.
- [55] Yu, C.-F. The isomorphism classes of abelian varieties of CM-type. *J. of Pure and Applied Algebra* 187, 2004, 305–319.
- [56] Zarhin, Y. Need to fill in.