

CM lifting of abelian varieties

Ching-Li Chai
Dept. of Math
Univ. of Pennsylvania
Philadelphia, PA 19104
chai@math.upenn.edu

Brian Conrad
Dept. of Math
Stanford Univ.
Stanford, CA 94305
conrad@math.stanford.edu

Frans Oort
Dept. of Math
Univ. of Utrecht
Utrecht, Netherlands
f.oort@uu.nl

July 18, 2009

§1. Introduction

An abelian variety A defined over a finite field \mathbb{F}_q admits sufficiently many complex multiplications, as Tate showed in [27]. For some details about complex multiplication, see §1.1. Is A the reduction of an abelian variety with sufficiently many complex multiplications in characteristic zero? We formulate several versions of this “CM-lifting problem” in §1.2. Honda proved that for some finite extension $\mathbb{F}_{q'}$ of \mathbb{F}_q there is an isogeny $A \otimes \mathbb{F}_{q'} \sim B$ over $\mathbb{F}_{q'}$ to an abelian variety B which admits a CM-lifting in the sense of the lifting problem (CML) in §1.2. By [23], in many cases such an isogeny is necessary: there are abelian varieties over $\overline{\mathbb{F}}_p$ which do not admit a CM-lifting.

In this paper we consider some obstructions which can be used to study various aspects of CM-lifting problems, especially what we will call the *residual reflex condition* (see §1.3–§1.5). In §2 we show that CM-lifting up to isogeny is possible over \mathbb{F}_q if the residual reflex obstruction is avoided in the strongest sense. In §3 we give counterexamples to the existence of CM-lifts up to isogeny over a normal local domain as in the lifting problem (NI) in §1.2. The main result of this paper (stated in §1.6) is that the residual reflex condition is the only obstruction to the lifting problem (NI).

(1.1) Complex multiplication

Let B be an abelian variety of dimension $g > 0$ over a field K . Its endomorphism algebra $\text{End}^0(B) = \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(B)$ is a finite-dimensional semisimple \mathbb{Q} -algebra in which every commutative semisimple subalgebra has degree at most $2g$ over \mathbb{Q} . If there is such a subalgebra $P \subseteq \text{End}^0(B)$ with $[P : \mathbb{Q}] = 2g$ then we say that B has *sufficiently many complex multiplications* (over K). The decomposition $P = \prod L_j$ into a product of fields induces a K -isogeny $B \sim \prod B_j$ where P acts (in the isogeny category over K) on each B_j through the quotient L_j , with $[L_j : \mathbb{Q}] = 2 \cdot \dim(B_j)$. We therefore focus on the case when $P = L$ is a field. Let i denote the embedding $L \hookrightarrow \text{End}^0(B)$; we call the pair (B, i) a *CM abelian variety* and we call i a *CM-structure* on B (over K); we also say that L is the *field of complex multiplication* of the pair (B, i) . In general, the subring $i^{-1}(\text{End}(B)) \subseteq L$ is an order in the ring of integers \mathcal{O}_L of L . For any CM abelian variety (B, i) over K , B is isotypic over K (i.e., there is a K -isogeny $B \sim B_0^e$ where B_0 is a K -simple abelian variety) and the unique K -simple factor B_0 of B also admits a structure of CM abelian variety over K .

The case of most interest is when L is a CM field because if B is K -simple and admits a

CM structure over K then $\text{End}^0(B)$ contains a CM maximal commutative subfield (necessarily of degree $2g$ over \mathbb{Q}) [31, 2.2]. For a K -simple B endowed with a CM-structure over K , if $\text{char}(K) = 0$ then the endomorphism algebra $\text{End}^0(B)$ is commutative, so it is a CM field. However, in positive characteristic it can happen (e.g., for absolutely simple 3-folds) that $\text{End}^0(B)$ is a non-commutative division algebra and there exists a maximal commutative subfield $P \subset \text{End}^0(B)$ which is not a CM field. Tate's work on endomorphism algebras of abelian varieties over finite fields ([27], [29]) implies that if K is finite then every (nonzero) isotypic abelian variety over K admits a CM-structure (over K). It is therefore natural to consider a CM abelian variety (B, i) over a finite field such that the field of complex multiplication L of (B, i) is a CM field, and to ask if (B, i) can be lifted to a CM abelian variety in characteristic 0. (The analogous, and perhaps more natural, question can be posed when L is instead a product $P = \prod L_j$ of CM fields, but this question is no more general if taken up to isogeny because the idempotents of such a P decompose any lifting compatibly with the associated isogeny decomposition $\prod B_j$ of B .)

It can happen that B is defined over a field $K \supseteq \mathbb{F}_p$ and $B \otimes_K \overline{K}$ cannot be defined over any finite subfield of \overline{K} yet B admits sufficiently many complex multiplications over K . Such a CM abelian variety over K does not admit a CM lifting to characteristic zero in the sense of the lifting problem (CML) in §1.2. However, by a theorem of Grothendieck (see [22]) the isogeny class of $B \otimes_K \overline{K}$ admits a member that can be defined over a finite subfield of \overline{K} .

(1.2) *Lifting problems*

Let \mathbb{F}_q be a finite field of size q , and let B be an abelian variety of dimension $g > 0$ over \mathbb{F}_q . Assume that B is isotypic over \mathbb{F}_q (which we have noted is necessary and sufficient in order that B admit a CM-structure over \mathbb{F}_q). Let B_K denote the scalar extension of B over an extension field $K \supset \mathbb{F}_q$. Consider the following five assertions concerning the existence of a CM-lifting of B .

- (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 an action (in the isogeny category over R) by a CM field L with $[L : \mathbb{Q}] = 2g$, and an isomorphism $\phi : A \otimes_R \mathbb{F}_q \simeq B$ 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 $A \otimes_R \mathbb{F}_q \sim B$ 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.

By expressing R as a direct limit of local subrings, 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 with an arbitrary unspecified extension of \mathbb{F}_q . In [23, Thm. B], for every prime p and every $g > 2$ we find examples of a g -dimensional abelian variety over $\mathbb{F} := \overline{\mathbb{F}}_p$ which does not satisfy the evident variant of (CML) using the residue field \mathbb{F} . Hence, (R) does not hold in general; that is, an isogeny is necessary in general.

On the other hand, results of Honda and Tate imply that (NIR) holds with R a p -adic integer ring and with $L \subseteq \text{End}^0(B)$ any CM subfield such that $[L : \mathbb{Q}] = 2g$. (See the beginning of §2 for a review of this implication.) By standard arguments that we omit, in the formulation of (I) there is no loss of generality in requiring R to be a complete local noetherian domain with residue field \mathbb{F}_q . For such R , every maximal ideal \mathfrak{m} of $R[1/p]$ has residue field $R[1/p]/\mathfrak{m}$ of finite degree over the fraction field of $W(\mathbb{F}_q)$ (by [14, 7.1.9], for example), and so by replacing R with its image in (the valuation ring of) $R[1/p]/\mathfrak{m}$ we see that R can even be taken to be an order with residue field \mathbb{F}_q in a p -adic integer ring. However, the finite residue field of R may increase after normalization. For this reason, on the one hand, (NI) is a priori a stronger property than (I). On the other hand, (NI) is a natural condition to consider because abelian schemes over normal base schemes have the pleasant property that homomorphisms between generic fibers extend (uniquely) over the entire base. We do not have a satisfactory understanding of (I), but in §2 we use deformation theory to give a sufficient criterion for it to hold. More interesting is that in §3 we use this criterion together with an arithmetic obstruction (explained in §1.3–§1.5) to give absolutely simple examples in which (I) holds but (NI) fails.

An interesting special case of (NI) is when the normal base ring R is a p -adic integer ring. Let us briefly explain why this is also essentially the general case; we only sketch the idea since it is not logically necessary in what follows. Recall that CM abelian varieties in characteristic 0 do not vary in positive-dimensional continuous families, in the sense that any CM abelian variety over an algebraically closed field k of characteristic zero descends to a number field $M \subseteq k$. Since such a descent has potentially good reduction at all finite places of M , if D is the universal deformation ring for a polarized CM abelian variety over a finite field \mathbb{F}_q (with deformations required to admit a compatible action by a fixed CM order) then the Zariski closure in $\text{Spec}(D)$ of every irreducible component of $\text{Spec}(D[1/p])$ (with its reduced structure) has the form $\text{Spec}(\Gamma)$ for a domain Γ that is finite flat over $W(\mathbb{F}_q)$. Suppose that (NI) holds for some B over \mathbb{F}_q using a lifting \mathcal{B}' of an \mathbb{F}_q -isogenous B' over a characteristic-0 complete local normal noetherian domain R with residue field \mathbb{F}_q . There is a polarization of the generic fiber of \mathcal{B}' over R , and by the normality of R this extends to an isogeny $\lambda : \mathcal{B}' \rightarrow \mathcal{B}'^t$ over R that is necessarily a polarization. This defines a natural local $W(\mathbb{F}_q)$ -algebra map $D \rightarrow R$ from a deformation ring D as above that is attached to B' equipped with its induced polarization and CM-structure from \mathcal{B}' . The image D_1 of D in R is finite flat over $W(\mathbb{F}_q)$, and by normality of R the normalization \tilde{D}_1 of D_1 is a local subring of R . Hence, \tilde{D}_1 has residue field \mathbb{F}_q , so (NI) holds for B using \tilde{D}_1 . In other words, if (NI) holds for B over \mathbb{F}_q then up to applying an \mathbb{F}_q -isogeny to B the appropriate universal deformation ring has a characteristic-0 component whose normalization is a p -adic integer ring with residue field \mathbb{F}_q .

(1.3) A residual obstruction

We will show in §2 via deformation theory that (I) is satisfied using any CM subfield $L \subseteq \text{End}^0(B)$ such that $[L : \mathbb{Q}] = 2g$ and $\kappa_v = \mathbb{F}_p$ for all p -adic places v of L (provided that such a subfield L exists, which we exhibit in some interesting examples in §3.5). We do not

know a necessary and sufficient criterion for (I) to hold, or if perhaps (I) holds in all cases. Our understanding of (NI) is much more satisfactory, as we now explain. The condition (NI) is subtle because there is an arithmetic obstruction to it coming from classical CM-theory. To explain this obstruction, fix an isotypic abelian variety B over \mathbb{F}_q with dimension $g > 0$. Let R be a local normal domain with characteristic 0 and residue field \mathbb{F}_q , and let A be an abelian scheme over R with relative dimension g equipped with an action (in the isogeny category over R) by a CM field L with $[L : \mathbb{Q}] = 2g$. Also assume that $A \otimes_R \mathbb{F}_q$ is isogenous to B over \mathbb{F}_q . By direct limit arguments, we can arrange that R is essentially of finite type over \mathbb{Z} , so it is excellent. Thus, we can replace R with its completion without losing the normality hypothesis (and this does not change the residue field). Since $M = \text{Frac}(R)$ has characteristic 0, the action on A over R by an order in \mathcal{O}_L uniquely extends to an M -linear action by L on the g -dimensional tangent space $T_0(A_M)$. By classical CM-theory, this action viewed over an algebraic closure \overline{M} decomposes into eigenlines on which L acts through a set Φ of g distinct embeddings of L into \overline{M} . This pair (L, Φ) is a CM type; i.e., Φ is a set of representatives for $\text{Hom}_{\text{ring}}(L, \overline{M})$ modulo the action on the CM field L by its intrinsic complex conjugation. We may of course view Φ as a subset of $\text{Hom}_{\text{ring}}(L, \overline{\mathbb{Q}_p})$, where $\overline{\mathbb{Q}_p}$ is the algebraic closure of \mathbb{Q}_p inside of \overline{M} . (This is also called a *p -adic CM type* to emphasize that its target is $\overline{\mathbb{Q}_p}$, so every $\phi \in \Phi$ induces a p -adic place on L .)

Associated to the p -adic CM type Φ for L there is the reflex field $E \subseteq \overline{\mathbb{Q}_p}$ of finite degree over \mathbb{Q} . This is the minimal subfield of M over which the linear action of L on the M -vector space $T_0(A_M)$ can be defined; it is the subfield of M generated by the traces of the action of all $\xi \in L$. Equivalently, if we let $\overline{\mathbb{Q}}$ denote the algebraic closure of \mathbb{Q} in $\overline{\mathbb{Q}_p}$ then $\text{Gal}(\overline{\mathbb{Q}}/E)$ is the subgroup of elements of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ stabilizing the subset $\Phi \subseteq \text{Hom}_{\text{ring}}(L, \overline{\mathbb{Q}})$. By normality of R , the inclusion of fields $E \subseteq M$ implies the inclusion of rings $\mathcal{O}_E \subseteq R$. But R is local with residue characteristic p , so its maximal ideal contracts back to a prime ideal \mathfrak{p} of \mathcal{O}_E over p . Note that the \mathfrak{p} -adic place on E is also induced by the inclusion of E into $\overline{\mathbb{Q}_p}$ due to the definition of E in terms of (L, Φ) .

By the construction of \mathfrak{p} in terms of R we see that $\mathcal{O}_E/\mathfrak{p}$ occurs as a subfield of the residue field \mathbb{F}_q of R . Thus, if (NI) holds for B over \mathbb{F}_q using some CM field $L \subseteq \text{End}^0(B)$ then there is a p -adic CM type Φ on L whose associated reflex field $E \subseteq \overline{\mathbb{Q}_p}$ has residue field at the induced place over p that is not “too large” in the sense that it can be embedded into \mathbb{F}_q . This is an arithmetic restriction on the p -adic CM type Φ .

(1.4) *A slope obstruction*

There is a further restriction on the p -adic CM type

$$\Phi \subseteq \text{Hom}_{\text{ring}}(L, \overline{\mathbb{Q}_p}) \subseteq \text{Hom}_{\text{ring}}(L, \overline{M})$$

that does not require normality of the complete local noetherian domain R (and so is a necessary condition on CM-types arising in (I) when R there is complete), as follows. Since L is its own centralizer in $\text{End}^0(B)$, and $\text{End}(B) \cap L$ is an order in \mathcal{O}_L , there is a unique element $\text{Fr}_{B,q} \in \mathcal{O}_L$ acting on B by the q -Frobenius endomorphism. Assume that there is an L -linear \mathbb{F}_q -isogeny between B and $A_0 = A \otimes_R \mathbb{F}_q$ for some A over R as in (I) with R noetherian and complete. This L -linear isogeny is compatible with q -Frobenius endomorphisms, so $\text{Fr}_{A_0,q} \in \mathcal{O}_L$ is equal to $\text{Fr}_{B,q}$. The *Shimura–Taniyama formula* for A relates the factorization of $\text{Fr}_{A_0,q} \mathcal{O}_L = \text{Fr}_{B,q} \mathcal{O}_L$ to the p -adic CM-type $\Phi \subseteq \text{Hom}_{\text{ring}}(L, \overline{\mathbb{Q}_p}) = \text{Hom}_{\text{ring}}(L, \overline{M})$ arising

from the L -action on $T_0(A_M)$: for each p -adic place v on L ,

$$\frac{\text{ord}_v(\text{Fr}_{B,q})}{\text{ord}_v(q)} = \frac{\#\{\phi \in \Phi : \phi \text{ induces } v \text{ on } L\}}{[L_v : \mathbb{Q}_p]}, \quad (1)$$

the choice of normalization of ord_v cancels out on the left side, and the right side is independent of the choice of $\overline{\mathbb{Q}_p}$. The ratios on the left side (as v varies) are called the *slopes* of B (over \mathbb{F}_q). More generally, if C is an abelian variety over \mathbb{F}_q with $q = p^f$ and if $F_C \in \mathbb{Z}[T]$ is the associated characteristic polynomial of $\text{Fr}_{C,q}$ then as λ_i varies through the roots of F_C in an algebraic closure $\overline{\mathbb{Q}_p}$ of \mathbb{Q}_p , the numbers $\text{ord}_p(\lambda_i)/f$ (usually counted with multiplicity) are called the *slopes* of C over \mathbb{F}_q ; here, ord_p is normalized by the condition $\text{ord}_p(p) = 1$. Obviously the formation of the slopes is invariant under isogeny and finite extension of the base field.

In the case that R is a p -adic integer ring, the formula (1) was first proved by Shimura and Taniyama using global arguments, and a local proof was given by Tate using p -divisible groups [29, §5]. The role of a Dedekind base in these proofs is to make the CM-order become maximal upon passing to an isogenous abelian scheme. That is, for Dedekind R , an abelian scheme A with an action by L in the isogeny category over R admits an isogeny to an abelian scheme A' over R on which the induced L -action in the isogeny category arises from an action of \mathcal{O}_L on the abelian scheme A' . Difficulties with R -flatness of scheme-theoretic closure in the non-Dedekind case make it unclear if such an A' can be found for general R . To handle all cases with $\dim(R) = 1$, let κ be the residue field of the R -finite normalization \tilde{R} of R and let $e = [\kappa : \mathbb{F}_q] \geq 1$. Clearly $\text{Fr}_{B_\kappa, \# \kappa} = \text{Fr}_{B,q}^e$ in \mathcal{O}_L since κ has size q^e ; hence the Shimura–Taniyama formula for $A \otimes_R \tilde{R}$ (equivalently, B_κ) implies the same for A (equivalently, B).

The general case can be reduced to the case of a 1-dimensional base by using an argument with universal deformation rings similar to what was done at the end §1.2, but here is a more concrete argument via spreading out and specialization. Let M denote the fraction field of R , $\mathcal{O} \subseteq \mathcal{O}_L$ an order that acts on A over R , and $\Gamma \subseteq \overline{\mathbb{Q}_p}$ a p -adic integer ring that is large enough to contain $\phi(\mathcal{O}_L)$ for all $\phi \in \Phi$. By applying standard descent and spreading arguments to the eigenline decomposition of $T_0(A) \otimes_R \overline{M}$ over \overline{M} via Φ , there is a nonzero $r \in R$ and a Γ -subalgebra $R' \subseteq \overline{M}$ that is finite étale over $R[1/r]$ and contains Γ such that $T_0(A) \otimes_R R'$ decomposes into a direct sum of free R' -modules of rank 1 on which \mathcal{O} acts by the maps $\phi : \mathcal{O} \rightarrow \Gamma \subseteq R'$. We can assume that $p|r$ in R , so $\text{Spec}(R[1/r])$ is a dense open subscheme of $\text{Spec}(R[1/p])$. Since $\text{Spec}(R[1/p])$ is Jacobson (e.g., due to [14, 7.1.9] and the Jacobson property of affinoid algebras [4, 5.2.6/3]), we can therefore choose a maximal ideal $\mathfrak{n} \in \text{MaxSpec}(R[1/p])$ that does not contain r . Let \mathfrak{p} be the corresponding prime ideal of R .

The local noetherian quotient domain $R_0 = R/\mathfrak{p}$ is clearly contained in the valuation ring of the finite extension $R_0[1/p] = R[1/r]/\mathfrak{n}$ of $\text{Frac}(W(\mathbb{F}_q))$, so it is an order in a p -adic integer ring. The quotient R'/\mathfrak{p} is finite étale over R_0 , so upon choosing a local factor ring of R'/\mathfrak{p} we see that $A \bmod \mathfrak{p}$ over R_0 equipped with its action by \mathcal{O} has CM-type that is naturally identified with Φ and has special fiber A_0 over \mathbb{F}_q (compatibly with \mathcal{O} -actions). Hence, the Shimura–Taniyama formula for A over R follows from the settled case of the formula for $A \bmod \mathfrak{p}$ over the 1-dimensional R_0 .

(1.5) Residual reflex condition

The considerations in §1.3–§1.4 show that if (NI) holds for an abelian variety B over \mathbb{F}_q with dimension $g > 0$, then there is a CM subfield $L \subseteq \text{End}^0(B)$ with $[L : \mathbb{Q}] = 2g$ and a p -adic CM type $\Phi \subseteq \text{Hom}_{\text{ring}}(L, \overline{\mathbb{Q}_p})$ such that (L, Φ) satisfies the following *residual reflex condition*:

- (i) The slopes of B are given in terms of (L, Φ) by the Shimura–Taniyama formula (1) in §1.4.
- (ii) Let $E \subseteq \overline{\mathbb{Q}}_p$ be the reflex field attached to (L, Φ) , and let v be the induced p -adic place of E . The residue field κ_v of $\mathcal{O}_{E,v}$ can be realized as a subfield of \mathbb{F}_q .

For example, if $g = 1$ then p splits in L if and only if the elliptic curve B is ordinary; it is straightforward to check that the residual reflex condition is satisfied for one choice (resp. both choices) of Φ when B is ordinary (resp. supersingular). That is, for elliptic curves over finite fields the residual reflex condition can be satisfied for any imaginary quadratic subfield of the endomorphism algebra.

We do not consider (i) in the residual reflex condition to be a serious constraint because the proof that (NIR) holds (which we review at the beginning of §2) shows that any CM subfield $L \subseteq \text{End}^0(B)$ with $[L : \mathbb{Q}] = 2g$ admits a p -adic CM type Φ for which (i) holds. Condition (ii) is more interesting because in §3.5 we use Honda–Tate theory to give absolutely simple examples such that $L = \text{End}^0(B)$ is a CM field of degree $2g$ and every p -adic CM type Φ on L satisfying the Shimura–Taniyama formula violates (ii). Moreover, we show that these examples satisfy (I). Thus, the (second part of the) residual reflex condition is a nontrivial obstruction to the validity of (NI) for a given triple (B, L, Φ) over \mathbb{F}_q , and this obstruction is eliminated by passing to a finite extension $\mathbb{F}_{q'} \supseteq \mathbb{F}_q$ if and only if $\mathbb{F}_{q'}$ is large enough to contain the residue field κ_v as in (ii).

In these absolutely simple counterexamples to (NI) that satisfy (I), B is an ℓ -dimensional abelian variety over \mathbb{F}_p with two distinct slopes over \mathbb{F}_p , where $\ell \geq 5$ is an arbitrary prime and p lies in a certain non-empty set of congruence classes depending on ℓ .

It is natural to ask whether there are obstructions to (NI) other than the residual reflex condition. We show in §5 that the combinatorial residual reflex condition is the only obstruction for (NI). This amounts to a refinement of Honda’s result that (NIR) holds in all cases, and it is recorded in Proposition 5.4, the main result of this paper. In terms of the above terminology, the result is this:

(1.6) Theorem *Let B be an abelian variety of dimension $g > 0$ over \mathbb{F}_q and let $L \subseteq \text{End}^0(B)$ be a CM field with $[L : \mathbb{Q}] = 2g$. Let $\Phi \subseteq \text{Hom}_{\text{ring}}(L, \overline{\mathbb{Q}}_p)$ be a p -adic CM type, and let $E \subseteq \overline{\mathbb{Q}}_p$ be the associated reflex field. Assume that (L, Φ) satisfies the residual reflex condition in §1.5.*

There exists a finite extension E'/E inside of $\overline{\mathbb{Q}}_p$, a g -dimensional abelian variety A over E' with good reduction at the p -adic place v' on E' induced by $\overline{\mathbb{Q}}_p$, and an inclusion $L \hookrightarrow \text{End}^0(A)$ with associated p -adic CM-type Φ such that the reduction of A at v' is L -linearly isogenous to B over an isomorphism of finite fields $\kappa_{v'} \simeq \mathbb{F}_q$. In particular, B satisfies (NI) using a lifting of the L -action over a p -adic integer ring with residue field \mathbb{F}_q .

The main ingredient in the proof is a purely arithmetic result (see Theorem 4.11) that gives a procedure to modify algebraic Hecke characters. Since the theory of complex multiplication tells us which algebraic Hecke characters comes from abelian varieties with complex multiplication (see Theorem 5.2), the algebraic Hecke character produced by Theorem 4.11 gives us a CM abelian variety over a number field E'/E , and we show that this is a CM-lifting of B (up to \mathbb{F}_q -isogeny) as required in Theorem 1.6. Note that the choice of isomorphism $\kappa_{v'} \simeq \mathbb{F}_q$ does not matter, since B is L -linearly \mathbb{F}_q -isogenous to $B^{(p)}$ via the relative Frobenius isogeny (and the natural isomorphism $B^{(q)} \simeq B$ is L -linear). In the final section of the paper we give an alternative proof of Theorem 1.6 that uses a local analogue of Theorem 4.11 (see

Lemma 6.1) but replaces the global theory of complex multiplication with local arguments resting on p -divisible groups and p -adic Hodge theory. We prefer the global argument because it is more explicit about the number field over which a given abelian variety over a finite field can be lifted.

The preceding considerations, including the formulation of the residual reflex condition, can be generalized to the case of abelian varieties with sufficiently many complex multiplications by a CM-algebra (i.e., a product of finitely many CM fields). We leave it to the reader to give a precise statement of this generalization because the proofs are immediately reduced to the case when the CM-algebra is a CM field.

(1.7) Acknowledgments and Notation

The authors are grateful to the 2006 Spring School on abelian varieties in Amsterdam where the initial work took place, and to Johan de Jong, James Milne, Ben Moonen, and René Schoof for helpful discussions. The work of the first two authors was partially supported by NSF grants DMS-0400482 and DMS-0600919 respectively, and the second author is very grateful to Columbia University for its generous hospitality during a sabbatical visit.

We write \mathbb{A}_L to denote the adèle ring of a number field L , $\mathbb{A}_{L,f}$ to denote the factor ring of finite adèles, and \mathbb{A} and \mathbb{A}_f in the case $L = \mathbb{Q}$. The Artin maps of local and global class field theory are taken with the arithmetic normalization, which is to say that local uniformizers are carried to arithmetic Frobenius elements. (We make this choice so that uniformizers correspond to Frobenius endomorphisms in the Main Theorem of complex multiplication.) The global reciprocity map for a number field L is denoted $\text{rec}_L : \mathbb{A}_L^\times / L^\times \rightarrow \text{Gal}(L^{\text{ab}}/L)$, and its composition with the projection $\mathbb{A}_L^\times \rightarrow \mathbb{A}_L^\times / L^\times$ is denoted r_L ; for a local field F we write r_F to denote the reciprocity map $F^\times \rightarrow \text{Gal}(F^{\text{ab}}/F)$.

If v is a place of a number field L then L_v denotes the completion of L with respect to v ; $\mathcal{O}_{L,v}$ denotes the valuation ring of L_v in case v is non-archimedean, with residue field κ_v whose size is denoted q_v . For a place w of \mathbb{Q} we let $L_w = \prod_{v|w} L_v = \mathbb{Q}_w \otimes_{\mathbb{Q}} L$, and in case w is the ℓ -adic place for a prime ℓ we let $\mathcal{O}_{L,\ell} = \prod_{v|\ell} \mathcal{O}_{L,v} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{O}_L$ (with \mathcal{O}_L the integer ring of L).

If $R \rightarrow R'$ is a map of rings and X is an R -scheme then $X_{R'}$ and $X \otimes_R R'$ denote $X \times_{\text{Spec } R} \text{Spec } R'$; if $\sigma : K \simeq K$ is an automorphism of a field K and X is a K -scheme then X^σ denotes $X \otimes_{K,\sigma} K$. The dual of an abelian scheme A is denoted A^t . The cardinality of a finite set Σ is denoted $\#\Sigma$.

§2. Existence of CM-lifting up to isogeny

Let B be an isotypic abelian variety of dimension $g > 0$ over a finite field \mathbb{F}_q with size q that is a power of a prime p . We give a sufficient criterion for (I) to be satisfied by B . To do this, let B_1 be an \mathbb{F}_q -simple isogeny factor of B , so there is an \mathbb{F}_q -isogeny $B \sim B_1^e$ with some $e \geq 1$. Let D_1 denote the division algebra $\text{End}^0(B_1)$, so $\text{End}^0(B)$ is an $e \times e$ matrix algebra over D_1 . Honda–Tate theory describes the structure of D_1 , including the fact that its maximal commutative subfields have degree $2 \cdot \dim(B_1)$ over \mathbb{Q} . Hence, B_1 admits a CM-structure over \mathbb{F}_q , so B does as well. In particular, we can find a CM subfield $L \subseteq \text{End}^0(B)$ with $[L : \mathbb{Q}] = 2g$. Fix such an L , so there is an element $\pi \in \mathcal{O}_L$ whose action on B is the q -Frobenius endomorphism $\text{Fr}_{B,q}$. We claim that there exists a p -adic CM type Φ on L that

satisfies the Shimura–Taniyama formula: for each p -adic place v of L ,

$$\frac{\text{ord}_v(\pi)}{\text{ord}_v(q)} = \frac{\#\{\phi \in \Phi \mid \phi \text{ induces } v \text{ on } L\}}{[L_v : \mathbb{Q}_p]}.$$

This is proved in [29, §4] in the \mathbb{F}_q -simple case, and the proof works in the general CM case over a finite field. We fix such a Φ .

Since B is \mathbb{F}_q -isotypic, Tate’s work on isogenies among abelian varieties over finite fields [27] gives two results for B : (i) the common characteristic polynomial over \mathbb{Q} for the action of π on the Tate modules of B is a power of an irreducible polynomial f_π over \mathbb{Q} (necessarily the minimal polynomial of π over \mathbb{Q}), and (ii) B is \mathbb{F}_q -isogenous to any g -dimensional isotypic abelian variety over \mathbb{F}_q whose q -Frobenius is a zero of f_π . Moreover, these properties persist after replacing \mathbb{F}_q with any finite extension κ (and replacing π with $\pi^{[\kappa:\mathbb{F}_q]}$).

We now prove (NIR) for B . By [29, §3, Thm. 2] (which is stated in the simple case but holds in the isotypic case by the same proof), there exists a number field $F \subseteq \overline{\mathbb{Q}_p}$, a g -dimensional abelian variety A_1 over F with good reduction at the induced p -adic place v , an embedding of finite fields $\mathbb{F}_q \hookrightarrow \kappa_v$, and an action of \mathcal{O}_L on A_1 with associated p -adic CM type Φ such that the reduction \overline{A}_1 at v has q_v -Frobenius in \mathcal{O}_L given by the action of $\pi_v = \pi^{[\kappa_v:\mathbb{F}_q]} \in L$. (Here, $q_v = \#\kappa_v$.) Since \overline{A}_1 admits a CM-structure over \mathbb{F}_{q_v} , it is \mathbb{F}_{q_v} -isotypic. Thus, since $\dim(\overline{A}_1) = \dim(B)$ and B_{κ_v} satisfies $\text{Fr}_{B_{\kappa_v}, q_v} = \text{Fr}_{B, q}^{[\kappa_v:\mathbb{F}_q]} = \pi_v$, it follows from the results in [27] recalled above that \overline{A}_1 is κ_v -isogenous to B_{κ_v} . Such a κ_v -isogeny $\phi_1 : \overline{A}_1 \rightarrow B_{\kappa_v}$ may fail to be L -linear but it is certainly $\mathbb{Q}(\pi_v)$ -linear since it is compatible with q_v -Frobenius endomorphisms. Since the q_v -Frobenius generates the center of the endomorphism algebra of any isotypic abelian variety over κ_v , the Skolem–Noether theorem ensures that any two $\mathbb{Q}(\pi_v)$ -embeddings of L into the finite-dimensional central simple $\mathbb{Q}(\pi_v)$ -algebra $\text{End}^0(B_{\kappa_v})$ are related through conjugation by a unit. Hence, there is a self-isogeny $u \in \text{End}(B_{\kappa_v})$ such that $u \circ \phi_1$ is L -linear, and so by renaming this as ϕ_1 we may assume that ϕ_1 is L -linear. Hence, (NIR) holds for B using the extension κ_v of \mathbb{F}_q , the base ring $\mathcal{O}_{F,v}$, and the CM lifting given by A_1 whose CM-type is (L, Φ) .

We want to refine this construction via deformation theory to prove that (I) holds for B using the CM-type (L, Φ) as chosen above, but unfortunately we only see how to do this subject to a restriction on the behavior of p in L (given in Proposition 2.1 below). Let $\mathcal{O} = L \cap \text{End}(B)$ be the associated CM-order in \mathcal{O}_L . Since \mathcal{O}_L is a finite \mathcal{O} -algebra with the same fraction field as \mathcal{O} , it is easy to find an L -linear \mathbb{F}_q -isogeny $B \sim B'$ where B' has CM-order equal to \mathcal{O}_L . Thus, upon replacing B with B' it suffices to consider the case when $\mathcal{O} = \mathcal{O}_L$.

(2.1) Proposition *With notation and hypotheses as above, assume in addition to \mathcal{O}_L being the CM-order that $\mathcal{O}_L/\mathfrak{p} = \mathbb{F}_p$ for every prime \mathfrak{p} of L over p . There exists an order R in a p -adic integer ring and an abelian scheme A over R equipped with an action by \mathcal{O}_L having CM type (L, Φ) as above such that R has residue field \mathbb{F}_q and $A \otimes_R \mathbb{F}_q$ is \mathcal{O}_L -linearly isomorphic to B over \mathbb{F}_q . In particular, B satisfies (CML) and hence satisfies (I).*

Some hypothesis on L at p is required in this proposition, since otherwise Remark 3.4 gives counterexamples via a tangential obstruction (the Kottwitz invariant). Beware that this does not mean that such examples cannot satisfy (I), since we may just need to pass to another member of the L -linear \mathbb{F}_q -isogeny class (perhaps with non-maximal CM-order) to get the required lift over a possibly non-normal base.

PROOF. As above, choose a number field $F \subseteq \overline{\mathbb{Q}}_p$ with induced p -adic place w , a CM abelian variety A_1 over F with good reduction at w and CM-type (L, Φ) and CM order \mathcal{O}_L , and an \mathcal{O}_L -linear isogeny $\phi_1 : \overline{A}_1 \rightarrow B_{\kappa_w}$. (In particular, κ_w is endowed with a structure of extension of \mathbb{F}_q .) The kernel $\ker \phi_1$ is a finite \mathcal{O}_L -submodule scheme of the g -dimensional \overline{A}_1 . We claim that there is a (unique) nonzero ideal $I \subseteq \mathcal{O}_L$ such that $\ker \phi_1 = \overline{A}_1[I]$. This is obvious on ℓ -primary parts for $\ell \neq p$ since $T_\ell(\overline{A}_1)$ is an invertible module over $\mathcal{O}_{L,\ell} = \prod_{q|\ell} \mathcal{O}_{L,q}$. The case of p -primary parts requires more care because the (contravariant) Dieudonné module $\mathbb{D}(\overline{A}_1[p^\infty])$ is a module over $W(\kappa_w) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L,p}$ rather than over $\mathcal{O}_{L,p}$.

First, the Dieudonné module is an invertible module over $W(\kappa_w) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L,p}$. Indeed, since $[L : \mathbb{Q}] = 2g = \dim \overline{A}_1$ and $\mathbb{D}(\overline{A}_1[p^\infty])$ is \mathbb{Z}_p -flat, the invertibility may be checked after inverting p , where it follows from the faithfulness of the L_p -action on $\mathbb{D}(\overline{A}_1[p^\infty])[1/p]$ (using the injectivity aspect in the p -part of Tate's isogeny theory over finite fields) and the fact that the Frobenius endomorphism on the Dieudonné module is $\mathcal{O}_{L,p}$ -linear but semilinear over the action of the absolute Frobenius on $W(\kappa_w)$. To find the p -part of the required ideal $I \subseteq \mathcal{O}_L$ such that $\ker \phi_1 = \overline{A}_1[I]$, first note that $\mathbb{D}(\ker \phi_1)$ is a quotient of $\mathbb{D}(\overline{A}_1[p^\infty])$ as modules over the Dieudonné ring D_{κ_w} over $W(\kappa_w)$, so by $W(\kappa_w) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L,p}$ -module freeness of $\mathbb{D}(\overline{A}_1[p^\infty])$ the kernel of the projection to this quotient is $J \cdot \mathbb{D}(\overline{A}_1[p^\infty])$ for a uniquely determined ideal $J \subseteq W(\kappa_w) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L,p}$ that is invertible (since $\mathbb{D}(\ker \phi_1)$ has finite length over $W(\kappa_w)$). Since each local factor $\mathcal{O}_{L,p}$ of $\mathcal{O}_{L,p}$ has residue field \mathbb{F}_p , the factor $W(\kappa_w) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L,p}$ of $W(\kappa_w) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L,p}$ is a local unramified extension of $\mathcal{O}_{L,p}$. In particular, J uniquely descends to an invertible ideal $I_p \subseteq \mathcal{O}_{L,p}$. This provides the p -part of the desired ideal $I \subseteq \mathcal{O}_L$.

Let \mathcal{A}_1 denote the Néron model of A_1 over the complete local ring $\mathcal{O}_{F,w}$ of \mathcal{O}_F at w , so \mathcal{A}_1 is an abelian scheme over $\mathcal{O}_{F,w}$ and the \mathcal{O}_L -action on A_1 uniquely extends to an action on \mathcal{A}_1 . Since the algebraic localization $\mathcal{O}_{L,(\ell)}$ is a principal ideal domain for every rational prime ℓ , consideration of primary parts yields that the torsion subscheme $\mathcal{A}_1[I]$ is a finite flat $\mathcal{O}_{F,w}$ -subgroup scheme of \mathcal{A}_1 (even if I is not globally principal). Thus, $\mathcal{A}_2 = \mathcal{A}_1/(\mathcal{A}_1[I])$ is an abelian scheme over $\mathcal{O}_{F,w}$ endowed with a natural action by \mathcal{O}_L . Moreover, the special fiber $\overline{\mathcal{A}}_2$ of \mathcal{A}_2 is \mathcal{O}_L -linearly isomorphic to $\overline{A}_1/(\overline{A}_1[I]) = \overline{A}_1/(\ker \phi_1) \simeq B_{\kappa_w}$. Hence, by replacing A_1 with $A_1/(\mathcal{A}_1[I])$ we can arrange that ϕ_1 is even an isomorphism. That is, \mathcal{A}_1 is an \mathcal{O}_L -linear deformation of B_{κ_w} . A polarization λ_1 of \mathcal{A}_1 over $\mathcal{O}_{F,w}$ induces a polarization on B_{κ_w} , but to get such a λ_1 whose reduction over κ_w descends to B over \mathbb{F}_q it is convenient (and also useful for later purposes in Theorem 2.3) to construct polarizations that interact well with the \mathcal{O}_L -action in rather more general situations:

(2.2) Lemma *Let X be an abelian variety of dimension $g > 0$ over an arbitrary field k , and let L be a CM field of degree $2g$ over \mathbb{Q} equipped with an action of its integer ring \mathcal{O}_L on X over k . Let $L_0 \subseteq L$ be the maximal totally real subfield, and let \mathcal{O}_L act on the dual abelian variety X^t via composition of the dual action with complex conjugation on L .*

The \mathcal{O}_{L_0} -module $\mathrm{Hom}_{\mathcal{O}_L}^{\mathrm{sym}}(X, X^t)$ of symmetric \mathcal{O}_L -linear homomorphisms over k is invertible, and likewise the \mathcal{O}_L -module $\mathrm{Hom}_{\mathcal{O}_L}(X, X^t)$ of \mathcal{O}_L -homomorphisms over k is invertible over \mathcal{O}_L , and there are \mathcal{O}_L -linear k -polarizations $\lambda : X \rightarrow X^t$.

We emphasize that both in this lemma and later, whenever we consider the dual X^t of a CM abelian variety X with field of complex multiplication equal to a CM field L it is understood that *the induced CM-structure by L on X^t is defined by composing the dual action with complex conjugation on L* . This convention is compatible with double duality.

PROOF. First consider the \mathcal{O}_L -module $\mathrm{Hom}_{\mathcal{O}_L}(X, X^t)$ of \mathcal{O}_L -linear maps over k . The additive

self-map $h \mapsto h' := h^t \circ \iota_X$ of $\mathrm{Hom}_{\mathcal{O}_L}(X, X^t)$ (where $\iota_X : X \simeq X^{tt}$ is the canonical isomorphism) is semi-linear over complex conjugation on \mathcal{O}_L due to how the \mathcal{O}_L -action on X^t is defined, and its fixed set is the \mathcal{O}_{L_0} -module $\mathrm{Hom}_{\mathcal{O}_L}^{\mathrm{sym}}(X, X^t)$. Moreover, $h'' = h$ for all h (since ι_{X^t} is inverse to ι_X^t), so for the two invertibility claims it suffices to prove that $\mathrm{Hom}_{\mathcal{O}_L}(X, X^t)$ is an invertible \mathcal{O}_L -module. It is clear that $\mathrm{Hom}_{\mathcal{O}_L}(X, X^t)$ is a finite flat \mathcal{O}_L -module, and by elementary rank considerations with ℓ -adic Tate modules for $\ell \neq p$ we see that its rank is at most 1. Thus, invertibility is reduced to being nonzero.

Consider k with characteristic 0. For an algebraic closure \bar{k} of k , we can descend the CM abelian variety $X_{\bar{k}}$ (with its CM-structure) to a number field, so there is a finite Galois extension k'/k such that $X_{k'}$ with its CM-structure descends to a CM abelian variety (A, α) over a number field $F \subseteq k'$. The complex-analytic theory provides an L -linear polarization on a complex fiber of A (due to how we define the L -action on A^t), and this descends to the corresponding $\overline{\mathbb{Q}}$ -fiber of A , and so also to a finite Galois extension F'/F . Thus, by increasing k' to split F'/F we can find an L -linear polarization $\lambda' : X_{k'} \rightarrow X_{k'}^t$ of $X_{k'}$. The sum of the $\mathrm{Gal}(k'/k)$ -conjugates of the L -linear map λ' descends to the desired polarization over k , and in particular this is a nonzero symmetric map.

For k with characteristic $p > 0$ we will proceed in reverse, first proving that $\mathrm{Hom}_{\mathcal{O}_L}(X, X^t)$ is nonzero and then afterwards using this to infer the existence of an L -linear k -polarization. The center of $\mathrm{End}^0(X)$ is identified with a subfield $Z \subseteq L$, and its image $Z^* \subseteq L$ under complex conjugation is identified with the center of $\mathrm{End}^0(X^t)$ when using the action of L on X^t through duality and complex conjugation. Let $h : X \rightarrow X^t$ be a k -polarization. The associated Rosati involution on $\mathrm{End}^0(X)$ restricts to an involution (perhaps trivial) τ on the center Z . By positivity properties of the Rosati involution, it follows that either Z is totally real and τ is the identity or Z is a CM field and τ is its complex conjugation. Either way, $Z^* = Z$ inside of L and the Rosati involution is complex conjugation on Z . This says that h is Z -linear via the definition of the L -action on X^t . It also follows that the center of $\mathrm{End}^0(X^t)$ is the subfield Z of $L \subseteq \mathrm{End}^0(X^t)$. The finite-dimensional \mathbb{Q} -algebras $\mathrm{End}^0(X)$ and $\mathrm{End}^0(X^t)$ are simple \mathbb{Q} -algebras (by k -isotypicity of X) in which the center is $Z \subseteq L$, so the Z -linear h induces a Z -algebra isomorphism $\psi : \mathrm{End}^0(X) \simeq \mathrm{End}^0(X^t)$. This may not be L -linear, but we can use the Skolem–Noether theorem to find a unit $u \in \mathrm{End}^0(X)^\times$ such that composing ψ with conjugation by u is an L -algebra isomorphism. Thus, after replacing u with a nonzero integral multiple so it lies in $\mathrm{End}(X)$, $h \circ u$ is an \mathcal{O}_L -linear k -isogeny $X \rightarrow X^t$ (perhaps not a polarization). In this argument, $\mathrm{char}(k)$ is arbitrary.

Now we construct L -linear k -polarizations in positive characteristic. We can assume that k is finitely generated over \mathbb{F}_p , so k is the function field of a normal variety U over the finite field κ that is the algebraic closure of \mathbb{F}_p in k . By shrinking U we can arrange that the CM abelian variety X over k spreads out to a CM abelian scheme \mathcal{X} over U . Normality of U implies that every k -homomorphism $X \rightarrow X^t$ uniquely extends to a U -homomorphism $\mathcal{X} \rightarrow \mathcal{X}^t$, and so for a choice of closed point $u \in U$ we get a specialization map

$$\mathrm{Hom}_k(X, X^t) \rightarrow \mathrm{Hom}_{\kappa(u)}(\mathcal{X}_u, \mathcal{X}_u^t)$$

that is injective. This induces an injection between the invertible \mathcal{O}_L -modules of \mathcal{O}_L -linear homomorphisms, so this latter injection is a finite-index inclusion. Hence, if the case of finite fields is settled then for a choice of L -linear $\kappa(u)$ -polarization λ_u of \mathcal{X}_u over the finite field $\kappa(u)$ we can replace λ_u with a positive integral multiple so that it arises from an L -linear map $\lambda : X \rightarrow X^t$ over $k = \kappa(U)$. This is a polarization because its extension over U specializes to a polarization on some fiber (namely, over u).

It remains to construct an L -linear k -polarization of X when k is finite, and it suffices to do this after replacing k with a finite extension k' (either due to the same finite-index inclusion trick as above, or by using the more elementary Galois descent trick used in characteristic 0). By Honda's result that (NIR) holds, after making a finite extension on k we can therefore assume that there is an L -linear k -isogeny $f : X \rightarrow Y$ with Y the reduction of an abelian variety \mathcal{Y} with good reduction and CM by L over a p -adic field F with residue field k (but the CM-order for \mathcal{Y}_F is perhaps not \mathcal{O}_L). We can choose an L -linear F -isogeny $\mathcal{Y}_F \rightarrow \mathcal{Y}'_F$ such that \mathcal{Y}'_F has CM-order \mathcal{O}_L , and since \mathcal{O}_F is Dedekind this extends to an L -linear isogeny $\mathcal{Y} \rightarrow \mathcal{Y}'$ to an abelian scheme \mathcal{Y}' over \mathcal{O}_F with CM-order \mathcal{O}_L . We may compose f with the reduction of this latter isogeny to get to the case when Y has CM-order equal to \mathcal{O}_L . By functoriality properties of polarizations we can rename Y as X , which is to say that we can assume that X equipped with its \mathcal{O}_L -action is identified with the reduction of an abelian variety \mathcal{X}_F equipped with an \mathcal{O}_L -action over a p -adic field F with residue field k . Any L -linear F -polarization of \mathcal{X}_F has reduction on X that is the desired L -linear k -polarization. \square

To apply Lemma 2.2 in the proof of Proposition 2.1, let $\lambda_1 : A_1 \rightarrow A_1^t$ be an \mathcal{O}_L -linear F -polarization as in the setup preceding the statement of Lemma 2.2. Its F_w -fiber extends to an \mathcal{O}_L -linear homomorphism $\lambda_{1,w} : \mathcal{A}_1 \rightarrow \mathcal{A}_1^t$ over $\mathcal{O}_{F,w}$ that is a polarization. This reduces to an \mathcal{O}_L -linear polarization $\bar{\lambda}_1$ on B_{κ_w} . But the inclusion

$$\mathrm{Hom}_{\mathcal{O}_L}(B, B^t) \rightarrow \mathrm{Hom}_{\mathcal{O}_L}(B_{\kappa_w}, B_{\kappa_w}^t)$$

between invertible \mathcal{O}_L -modules must be a finite-index inclusion, so by replacing λ_1 with $n \cdot \lambda_1$ for some integer $n > 0$ we can assume that the polarization $\bar{\lambda}_1$ over κ_w descends to an \mathbb{F}_q -polarization λ_B of B . (This λ_B is also \mathcal{O}_L -linear, but that will not be needed.)

Consider the deformation functor $\mathrm{Def}(B, i_B, \lambda_B)$ of the polarized abelian scheme (B, λ_B) equipped with \mathcal{O}_L -action via the canonical inclusion $i_B : \mathcal{O}_L \rightarrow \mathrm{End}(B)$. This functor is the subfunctor of $\mathrm{Def}(B, \lambda_B)$ defined by requiring that the \mathcal{O}_L -action on B lifts (necessarily uniquely) to the deformation of B . It is a standard fact in the deformation theory of polarized abelian schemes that the deformation functor $\mathrm{Def}(B, i_B, \lambda_B)$ considered on the category of complete local noetherian $W(\mathbb{F}_q)$ -algebras (with residue field possibly larger than \mathbb{F}_q , such as κ_w) is represented by a complete local noetherian $W(\mathbb{F}_q)$ -algebra D with residue field \mathbb{F}_q .

The polarized abelian scheme over $\mathcal{O}_{F,w}$ provided by \mathcal{A}_1 equipped with its \mathcal{O}_L -action and polarization $\lambda_{1,w}$ (and residual isomorphism ϕ_1 giving the deformation structure with respect to (B, i_B, λ_B) over \mathbb{F}_q) is classified by a local $W(\mathbb{F}_q)$ -algebra homomorphism $f : D \rightarrow \mathcal{O}_{F,w}$. Let $R = D/\mathrm{Ker}(f)$, so R is an order with residue field \mathbb{F}_q in a p -integer ring contained in $\mathcal{O}_{F,w}$. The pullback to $\mathrm{Spec} R$ of the universal deformation, equipped with its pullback \mathcal{O}_L -action and residual isomorphism to B over \mathbb{F}_q , is the desired CM-lifting of (B, i_B) to characteristic 0 without increasing the residue field (and it has the same CM-type Φ as does \mathcal{A}_1). This completes the proof of Proposition 2.1. \square

We conclude this section by using Lemma 2.2 to prove a tangential necessary and sufficient criterion for the algebraicity of a formal abelian scheme with complex multiplication. This criterion is only used in our alternative local proof of Theorem 1.6 in §6.

(2.3) Theorem *Let R be a \mathbb{Z}_p -flat 1-dimensional complete local noetherian ring with residue characteristic p , and let \mathfrak{A} be a formal abelian scheme over R of relative dimension $g > 0$. Assume that the finite-dimensional \mathbb{Q} -algebra $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_R(\mathfrak{A})$ contains a commutative semisimple*

CM-subalgebra L with $[L : \mathbb{Q}] = 2g$. Then \mathfrak{A} is algebraizable if and only if the $R[1/p]$ -linear L -action on $T_0(\mathfrak{A})[1/p]$ is given by a CM-type over each geometric point of $\mathrm{Spec}(R[1/p])$. In such cases, the algebraization admits an ample line bundle giving rise to an L -linear polarization.

By using the deformation theory of formal modules, the examples discussed below in Remark 3.4 admit formal deformations \mathfrak{A} over p -adic integer rings R such that the tangential hypothesis in Theorem 2.3 is not satisfied, and so these are not algebraizable. This is interesting because the rigid-analytic generic fibers of such \mathfrak{A} are smooth, proper, connected rigid-analytic groups X over p -adic fields such that X admits complex multiplication in the evident sense but X is not algebraic (and does not become so after any finite extension on the base field). The details are left to the interested reader.

PROOF. The necessity of the tangential condition is a consequence of the complex-analytic theory of abelian varieties. Thus, we focus on sufficiency.

Step 1. Let us first reduce to the case when R is a domain. We can assume that R is reduced because R_{red} is \mathbb{Z}_p -flat and if $\mathfrak{A} \widehat{\otimes}_R R_{\mathrm{red}}$ admits a formally ample line bundle \mathcal{L} then by positivity of the residue characteristic there is an $m \geq 1$ (depending on the order of nilpotence of the nilradical of R) such that $\mathcal{L}^{\otimes p^m}$ lifts to a line bundle \mathfrak{N} on \mathfrak{A} . This lift is necessarily formally ample, and the associated formal polarization $\phi_{\mathfrak{N}}$ is L -linear if $\phi_{\mathcal{L}}$ is. Assuming the domain case is settled, we shall now induct on the number of irreducible components by a standard gluing argument along closed subschemes.

Let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ be the minimal primes of R , so $\cap \mathfrak{p}_i = (0)$. We may assume $n > 1$, as otherwise we are in the domain case that we are assuming is settled. For $J = \mathfrak{p}_1$ and $J' = \cap_{j>1} \mathfrak{p}_j$, the natural map $R \rightarrow (R/J) \times_{R/(J+J')} (R/J')$ is an isomorphism. (Note that R/J and R/J' are \mathbb{Z}_p -flat since R is \mathbb{Z}_p -flat.) We now check rather generally that if R is an adic noetherian ring and \mathfrak{X} is any proper flat formal R -scheme with algebraizable pullbacks to $\mathrm{Spf}(R/J)$ and $\mathrm{Spf}(R/J')$ for ideals $J, J' \subseteq R$ such that $R \simeq (R/J) \times_{R/(J+J')} (R/J')$ then \mathfrak{X} is algebraizable. Let X and X' be the respective proper flat algebraizations of $\mathfrak{X} \bmod J$ and $\mathfrak{X} \bmod J'$ over R/J and R/J' , so by formal GAGA there is a unique isomorphism between their pullbacks over $R/(J+J')$ respecting the identification of the formal completions of such pullbacks with $\mathfrak{X} \bmod (J+J')$. We can glue along this isomorphism to get a proper flat R -scheme Y , and by R -flatness it follows that the associated formal scheme \widehat{Y} over $\mathrm{Spf}(R)$ is the analogous gluing of $\widehat{X} = \mathfrak{X} \bmod J$ and $\widehat{X}' = \mathfrak{X} \bmod J'$. Since \mathfrak{X} is R -flat, this gluing of formal schemes is identified with \mathfrak{X} . Hence, Y is an algebraization of \mathfrak{X} . It is clear that this gluing argument behaves well with respect to polarizations in the case that \mathfrak{X} is a formal abelian scheme. Thus, we may suppose that R is a domain.

Step 2. We next reduce to the case when the 1-dimensional \mathbb{Z}_p -flat complete local noetherian domain R is a discrete valuation ring with algebraically closed residue field. By Lemma 2.2, applied to the isotypic factors of the special fiber \overline{A} of \mathfrak{A} over the residue field k (all of which are CM abelian varieties over k with CM-algebras given by the CM factor fields of L), we can choose an L -linear k -polarization $\phi_{\mathcal{L}} : \overline{A} \rightarrow \overline{A}^t$ arising from an ample line bundle \mathcal{L} on \overline{A} . Let I be an \mathfrak{m}_R -primary ideal admitting topologically nilpotent divided powers, such as pR if $p > 2$ or $4R$ if $p = 2$. Since R/I is 0-dimensional with residue characteristic p , if we replace \mathcal{L} with a suitable p -power then we can assume that $\phi_{\mathcal{L}}$ lifts to a homomorphism ϕ_0 over R/I . Let $R_n = R/I^{n+1}$ and $A_n = \mathfrak{A} \otimes_R R_n$ for $n \geq 0$. We claim that ϕ_0 over R_0 lifts to an R -homomorphism $\phi_\infty : \mathfrak{A} \rightarrow \mathfrak{A}^t$, thereby providing the required formally ample line bundle on \mathfrak{A} (namely, the $(1, \phi_\infty)$ -pullback of the formal Poincaré bundle).

Let $\Gamma = \mathfrak{A}[p^\infty]$ and $\Gamma' = \mathfrak{A}^t[p^\infty]$, and for $n \geq 0$ let Γ_n and Γ'_n denote the reductions

modulo I^{n+1} . Note that $R_n \rightarrow R_0$ has kernel I/I^{n+1} with canonical nilpotent divided powers. By the Serre–Tate theorem [15, 1.2.1], to make the desired R -lift of ϕ_0 it is equivalent to construct an R -lifting of the L -linear k -isogeny $\Gamma_0 \rightarrow \Gamma'_0$ induced by ϕ_0 on p -divisible groups. By Grothendieck–Messing theory and the divided power hypothesis on I , the data of the deformation Γ of Γ_0 is covariantly functorially encoded as a pair (D^0, D) where D is a finite projective R -module of rank $2g$ and D^0 is a finite projective R -submodule of rank g that is a direct summand. Explicitly, if we let D_n be the Lie algebra of the universal vector extension $E(\Gamma_n)$ of Γ_n by a vector group over R_n then $D_{n+1} \otimes_{R_{n+1}} R_n \simeq D_n$ for all $n \geq 0$ and D is the inverse limit of the D_n 's. The functoriality of D in Γ_0 is determined by that of each D_n via the above specification of divided-power structure on I . Also, $D^0 \subseteq D$ is the inverse limit of the subbundles $D_n^0 = \omega_{\Gamma_n^*} \subseteq D_n$ given by the cotangent spaces along the identity to the dual p -divisible groups Γ_n^* . There is a similar such pair (D'^0, D') for Γ' as a deformation of Γ'_0 , and the k -map ϕ_0 induces an R -linear map $[\phi_0] : D \rightarrow D'$. The existence of ϕ_∞ is equivalent to the condition that $[\phi_0]$ carries D^0 into D'^0 .

Since $D^0 \subseteq D$ and $D'^0 \subseteq D'$ are subbundles over $\text{Spec}(R)$ and R is a \mathbb{Z}_p -flat domain, it is equivalent to check the subbundle compatibility of $[\phi_0]$ after extending scalars to an algebraic closure \overline{Q} of the field $Q = \text{Frac}(R)$ of characteristic 0. In particular, it is harmless to replace ϕ_0 with $p^r \phi_0$ for any $r \geq 1$. By functoriality, the Q -linear map $[\phi_0]_Q : D_Q \rightarrow D'_Q$ is also L -linear. We claim that D_Q and D'_Q are invertible $Q \otimes_{\mathbb{Q}} L$ -modules and that the submodules D_Q^0 and D'^0_Q are spanned over \overline{Q} by the 1-dimensional eigenspaces for a common set of g embeddings $L \rightarrow \overline{Q}$. This will force $[\phi_0]_Q$ to carry D_Q^0 into D'^0_Q , as required.

The definitions of (D^0, D) and (D'^0, D') as well as the action on these pairs by CM-orders for Γ and $\Gamma' = \Gamma^*$ in L are intrinsic to the system of universal vector extensions of Γ_n and Γ'_n over $\text{Spec}(R_n)$ for all $n \geq 0$. We have thereby eliminated the need to pay attention to functoriality of these vector extensions with respect to the k -morphism ϕ_0 that we do not yet know to have a lifting, since we have reduced ourselves to some module-theoretic properties of (D^0, D) and (D'^0, D') that have nothing to do with ϕ_0 . By considering Q -ranks, invertibility of D_Q is equivalent to its faithfulness as a $Q \otimes_{\mathbb{Q}} L$ -module. Since R is a noetherian local domain of dimension 1 we can choose a local injection $R \rightarrow \mathcal{O}$ into a complete discrete valuation ring \mathcal{O} , so Q injects into $\text{Frac}(\mathcal{O}) = \mathcal{O}[1/p]$. The formation of the universal vector extension of a p -divisible group (over a base on which p is locally nilpotent) commutes with any base change, so it suffices to consider our linear algebra problems after the base change $\text{Spf}(\mathcal{O}) \rightarrow \text{Spf}(R)$. That is, we may assume that R is a discrete valuation ring, and we can also assume that the residue field k of R is algebraically closed. (Observe that this reduction step preserves the geometric tangential hypothesis whose sufficiency for algebraization we are trying to prove.)

Step 3. We now focus on proving that D_Q is an invertible $Q \otimes_{\mathbb{Q}} L$ -module (so we ignore D^0). We will use comparison isomorphisms between Dieudonné theory and crystalline cohomology after inverting p (to avoid restrictions on the absolute ramification degree). By [18, Ch. V, 2.1], there is a canonical $R/(p^{n+1})$ -linear isomorphism between the Lie algebras of the universal vector extensions of $\Gamma \bmod p^{n+1}$ and $\mathfrak{A} \bmod p^{n+1}$ for all $n \geq 0$, and this is compatible with change in n . But [17, Ch. I, 2.6.7, 3.2.3, 4.1.7, 4.2.1] gives a canonical $R/(p^{n+1})$ -linear isomorphism

$$\text{Lie}(E(\mathfrak{A} \bmod p^{n+1})) \simeq H_{\text{dR}}^1((\mathfrak{A}^t \bmod p^{n+1})/(R/(p^{n+1})))$$

compatibly with change in n , so passage to the inverse limit gives $D \simeq H_{\text{dR}}^1(\mathfrak{A}^t/R)$ due to the theorem on formal functions for hypercohomology of bounded C -linear complexes of coherent sheaves on a proper formal schemes over a complete local noetherian ring C . (This version

of the theorem on formal functions is easily deduced from the special case of cohomology of coherent sheaves on proper formal schemes given in [9, III₁, 3.4.4.].) Hence, we have a canonical Q -linear isomorphism

$$D_Q \simeq H_{\text{dR}}^1(\mathfrak{A}^t/R)[1/p] \simeq Q \otimes_W H_{\text{cris}}^1(\overline{A}^t/W), \quad (2)$$

where $W = W(k)$ and the final isomorphism comes from [3, (2.4.2)].

By using canonicity with respect the action on \mathfrak{A} by an order in L we see that the composite isomorphism (2) is $Q \otimes_{\mathbb{Q}} L$ -linear when using the L -action on $H_{\text{cris}}^1(\overline{A}^t/W)[1/p]$ defined via pullback of the dual of the L -action on \overline{A} in the isogeny category over k . Thus, the invertibility of D_Q over $Q \otimes_{\mathbb{Q}} L$ is equivalent to that of $H_{\text{cris}}^1(\overline{A}^t/W)[1/p]$ over $K_0 \otimes_{\mathbb{Q}} L$, where $K_0 = W[1/p]$. The comparison of classical contravariant Dieudonné theory and crystalline cohomology for abelian varieties [2, 2.5.5–2.5.7, 3.3.7, 4.2.14] naturally identifies the W -modules $H_{\text{cris}}^1(X/W)$ and $\mathbb{D}(X[p^\infty])^{(p)}$ for any abelian variety X over k , so our problem reduces to proving that $\mathbb{D}(X[p^\infty])[1/p]$ is an invertible $K_0 \otimes_{\mathbb{Q}} L$ -module for any such X of dimension g endowed with a CM-structure by L . But $K_0 \otimes_{\mathbb{Q}} L = K_0 \otimes_{\mathbb{Q}_p} L_p$ and the Frobenius operator on $\mathbb{D}(X[p^\infty])[1/p]$ is an L_p -linear automorphism that is semilinear over the absolute Frobenius automorphism of K_0 , so for K_0 -rank reasons it suffices to prove faithfulness of the K_0 -linear action by L_p . Since

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \text{Hom}_k(X_1, X_2) \rightarrow \text{Hom}_k(X_1[p^\infty], X_2[p^\infty])$$

is injective for any abelian varieties X_1 and X_2 over k and the Dieudonné functor on p -divisible groups over k is faithful, we are done with the proof of invertibility of D_Q and D'_Q over $Q \otimes_{\mathbb{Q}} L$.

Step 4. It remains to determine the $Q \otimes_{\mathbb{Q}} L$ -module structures of D_Q^0 and D'^0_Q . More precisely, when the invertible $Q \otimes_{\mathbb{Q}} L$ -modules D_Q and D'_Q are viewed over \overline{Q} , each \mathbb{Q} -algebra map $L \rightarrow \overline{Q}$ has a 1-dimensional eigenspace and the submodules D_Q^0 and D'^0_Q are each spanned over \overline{Q} by the half of these eigenlines. We have to show that the eigencharacters arising in these submodules coincide. By its construction, D^0 is the formal cotangent space of Γ^* along the identity, or equivalently of \mathfrak{A}^t along the identity. This latter cotangent space is naturally identified with the R -linear dual of $H^1(\mathfrak{A}, \mathcal{O}_{\mathfrak{A}})$ compatibly with the L -actions after inverting p (where L acts on $H^1(\mathfrak{A}, \mathcal{O}_{\mathfrak{A}})[1/p]$ via pullback of its given action on \mathfrak{A} in the isogeny category over R). Likewise, via the double duality isomorphism $(\mathfrak{A}^t)^t \simeq \mathfrak{A}$ of formal abelian schemes over R , D'^0_Q is identified with $H^0(\mathfrak{A}, \Omega_{\mathfrak{A}/R}^1)[1/p]$ as a $Q \otimes_{\mathbb{Q}} L$ -module where L acts through the complex conjugate of its given action on \mathfrak{A} in the isogeny category over R (due to how L acts on \mathfrak{A}^t). Thus, it suffices to show that when we view $H_{\text{dR}}^1(\mathfrak{A}/R)[1/p]$ as an invertible $Q \otimes_{\mathbb{Q}} L$ -module using the given L -action on \mathfrak{A} then complex conjugation on L swaps the eigencharacters arising on the two graded pieces $H^0(\mathfrak{A}, \Omega_{\mathfrak{A}/R}^1)[1/p]$ and $H^1(\mathfrak{A}, \mathcal{O}_{\mathfrak{A}})[1/p]$ of the Hodge filtration. By invertibility over $Q \otimes_{\mathbb{Q}} L$ and Q -rank considerations it is equivalent to check that there are no conjugate pairs arising in one of the graded parts, such as in $H^0(\mathfrak{A}, \Omega_{\mathfrak{A}/R}^1)[1/p]$. Passing to the Q -linear dual, we are reduced to checking that the eigencharacters arising for the L -action on $T_0(\mathfrak{A})[1/p]_{\overline{Q}}$ constitute a (\overline{Q} -valued) CM-type of L . But this is exactly the initial tangential hypothesis. \square

§3. CM-lifting to a normal domain up to isogeny: counterexamples

We give two classes of counterexamples to (NI), the second of which is more satisfying but the first of which is easier to explain.

(3.1) Supersingular counterexamples

Choose a prime number p such that $p \equiv 2, 3 \pmod{5}$, so p remains prime in $\mathbb{Q}(\mu_5)$. Consider an algebraic integer in $\mathbb{Q}(\mu_5)$ of the form $\pi = p\zeta_5$, where ζ_5 is a primitive fifth root of unity in $\mathbb{Q}(\mu_5)$. This is a p^2 -Weil number. By Honda–Tate theory there is (uniquely up to isogeny) an \mathbb{F}_{p^2} -simple abelian variety B over \mathbb{F}_{p^2} such that the center of $\text{End}^0(B)$ may be identified with $F := \mathbb{Q}[\pi] = \mathbb{Q}(\mu_5)$ via $\pi \mapsto \text{Fr}_{B,p^2}$. Moreover, the central division algebra $D = \text{End}^0(B)$ over F is split away from the unique p -adic place of F , so it is globally split and hence is equal to its center F . Thus,

$$2 \cdot \dim(B) = [F : \mathbb{Q}] \sqrt{[D : F]} = 4,$$

so $\dim(B) = 2$. Hence, the only CM-structure on B (up to choosing an isomorphism $\mathbb{Q}(\mu_5) \simeq \text{End}^0(B)$) is the canonical one provided by the action of $\mathbb{Q}(\mu_5)$.

(3.2) Lemma *The reflex field of every CM-type on $\mathbb{Q}(\mu_5)$ is non-canonically isomorphic to $\mathbb{Q}(\mu_5)$.*

PROOF. If L is a CM field that is Galois over \mathbb{Q} then any CM-type Φ on L has reflex field $E \subseteq \overline{\mathbb{Q}}$ that is contained in the canonical image of L in $\overline{\mathbb{Q}}$. But the reflex field of a CM-type is a CM field as well, so if in addition L has no proper CM subfield then $E \simeq L$. An example of such an L is $\mathbb{Q}(\mu_\ell)$ for a Fermat prime ℓ , such as $\ell = 5$. \square

(3.3) Corollary *For $p \equiv 2, 3 \pmod{5}$ and B over \mathbb{F}_{p^2} as above, no member of the \mathbb{F}_{p^2} -isogeny class of B can be lifted to an abelian scheme X over a normal local domain R with characteristic 0 and residue field \mathbb{F}_{p^2} such that the generic fiber of X has sufficiently many complex multiplications. In particular, B does not satisfy (NI).*

We can show that B over \mathbb{F}_{p^2} satisfies (CML) provided that $\text{End}(B)$ is the full ring of integers in the CM field $\text{End}^0(B) \simeq \mathbb{Q}(\mu_5)$, and so in general any B as above satisfies (I). The verification of this rests on a trick, so we omit it; note that $\mathbb{Q}(\mu_5)$ violates the hypotheses at p in the sufficient criterion for (CML) in Proposition 2.1.

PROOF. Assume that such an X exists, and let F be the fraction field of R . By faithfulness of reduction to the special fiber, we get an injection

$$\text{End}^0(X \otimes_R F) = \text{End}^0(X) \hookrightarrow \text{End}^0(B) = \mathbb{Q}(\mu_5)$$

into a quartic number field. (The initial equality holds because R is normal.) Hence, since $\dim(X \otimes_R F) = \dim(B) = 2$, the only way that $X \otimes_R F$ can have sufficiently many complex multiplications is if it has a CM-structure given by a lifting of the $\mathbb{Q}(\mu_5)$ -action on its special fiber (upon fixing an \mathbb{F}_{p^2} -isogeny between B and the special fiber of X , the choice of which does not matter since $\text{End}^0(B) = \mathbb{Q}(\mu_5)$ is commutative). We therefore assume that there exists such a lifted action of $\mathbb{Q}(\mu_5)$ on $X \otimes_R F$ in the isogeny category over F (or equivalently on X in the isogeny category over R).

Choose an algebraic closure \overline{F} of F and let Φ be the resulting p -adic CM-type on $\mathbb{Q}(\mu_5)$. The congruence conditions on p imply that there is a unique p -adic place on $\mathbb{Q}(\mu_5)$ and it is unramified over p . It follows that Φ satisfies the Shimura–Taniyama formula for B over \mathbb{F}_{p^2} . By Lemma 3.2, the reflex field of $(\mathbb{Q}(\mu_5), \Phi)$ is isomorphic to $\mathbb{Q}(\mu_5)$. Hence, this reflex field likewise admits a unique (and unramified) p -adic place, and so this place has residue field \mathbb{F}_{p^4} of degree 4 over \mathbb{F}_p . By the necessity of the residual reflex condition (since R is normal), the residue field of R contains \mathbb{F}_{p^4} . But the residue field of R is \mathbb{F}_{p^2} , so we have a contradiction and therefore no such X exists. \square

(3.4) Remark If we replace $\mathbb{Q}(\mu_5)$ with $\mathbb{Q}(\mu_\ell)$ for any Fermat prime $\ell \geq 5$ (so there is no proper CM subfield of $\mathbb{Q}(\mu_\ell)$ and $[\mathbb{Q}(\mu_\ell) : \mathbb{Q}] > 2$), then the preceding construction works over \mathbb{F}_{p^2} for any prime $p \neq \ell$ with $p \not\equiv \pm 1 \pmod{\ell}$ (so $p \pmod{\ell}$ in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ has order exceeding 2). In such examples, B is \mathbb{F}_{p^2} -simple with dimension $(\ell - 1)/2$ and endomorphism algebra $\mathbb{Q}(\mu_\ell)$ in which $\text{Fr}_{B, p^2} = \pi := p\zeta_\ell$ for a primitive ℓ th root of unity ζ_ℓ in $\mathbb{Q}(\mu_\ell)$. Thus, $\pi^\ell = p^\ell$, so over $\mathbb{F}_{p^{2\ell}}$ there is an isogeny between B and a power of a supersingular elliptic curve. Hence, these B 's are supersingular abelian varieties.

Consider the special case when p is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ and the CM order is $\mathbb{Z}[\mu_\ell]$. In this case the tangent space $T_0(B)$ of dimension $(\ell - 1)/2$ over \mathbb{F}_{p^2} is 1-dimensional over $\mathbb{Z}[\mu_\ell]/(p) \simeq \mathbb{F}_{p^{\ell-1}}$. Since complex conjugation on $\mathbb{Z}[\mu_\ell]$ induces an \mathbb{F}_{p^2} -automorphism of $\mathbb{F}_{p^{\ell-1}}$, the conclusion of Proposition 2.1 cannot hold for B over \mathbb{F}_{p^2} with $L = \mathbb{Q}(\mu_\ell)$ since the μ_ℓ -action on the tangent space in characteristic p forces the geometric tangential action in characteristic 0 to be given by a collection of eigencharacters that is stable under complex conjugation, contradicting the requirement to be a CM type.

(3.5) Counterexamples with two slopes

The preceding supersingular counterexamples to (NI) are not absolutely simple. We now give absolutely simple counterexamples. To make it easier to violate the necessary residual reflex condition we will work over \mathbb{F}_p . Fix an odd prime $\ell \geq 5$ and an integer r such that $1 < r < \ell/2$. We shall construct counterexamples to (NI) over \mathbb{F}_p that satisfy (CML) (and hence (I)) and are absolutely simple abelian varieties B of dimension ℓ over \mathbb{F}_p , with p satisfying some congruence conditions to be determined shortly. In these examples B will have slopes r/ℓ and $1 - r/\ell$, each with multiplicity ℓ .

Choose an imaginary quadratic field F whose discriminant is prime to ℓ (so in particular, F is linearly disjoint from $\mathbb{Q}(\mu_\ell)$ over \mathbb{Q}). Choose a prime $p \nmid \ell \cdot \text{disc}(F)$ such that $p \pmod{\ell}$ is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$, which is to say that p is inert in $\mathbb{Q}(\mu_\ell)$. Assume that p splits in F and that the two prime ideals \wp and $\bar{\wp}$ of \mathcal{O}_F over p are principal ideals. For example, if we consider F with class number 1 (i.e., $F = \mathbb{Q}(\sqrt{-D})$ with $D = 1, 2, 3, 7, 11, 19, 43, 67, 163$, so at most one such F is ruled out by the condition $\ell \nmid \text{disc}(F)$), then the conditions on p say that it lies in some non-empty set of congruence classes modulo $\ell \cdot \text{disc}(F)$; in the special case $\ell = 5$ and $F = \mathbb{Q}(\sqrt{-1})$, the condition is $p \equiv 13, 17 \pmod{20}$.

Write $\wp = \alpha\mathcal{O}_F$. Let $L = F(u)$ be an extension field of F such that $u^\ell = \alpha^r \bar{\alpha}^{\ell-r} = p^r \bar{\alpha}^{\ell-2r}$. The extension L/F is unambiguous because $X^\ell - \alpha^r \bar{\alpha}^{\ell-r} \in F[X]$ is irreducible (as it is even \wp -adically irreducible). Likewise, $F = \mathbb{Q}(u^\ell)$, so $L = \mathbb{Q}(u)$. Observe that the algebraic integer u is a p -Weil number, and $L = \mathbb{Q}(u)$ is a CM field containing the imaginary quadratic field F in which p is split. Since $(p/u)^\ell = p^r \alpha^{\ell-2r}$, we see that L/F is totally ramified at both primes \wp and $\bar{\wp}$ of \mathcal{O}_F over p (so \mathcal{O}_L has residue field \mathbb{F}_p at all primes over p). By Honda–Tate theory there is an \mathbb{F}_p -simple ℓ -dimensional abelian variety B over \mathbb{F}_p endowed with an action by L in the isogeny category over \mathbb{F}_p such that $\text{Fr}_{B, p} = u$. This abelian variety has two distinct slopes, namely r/ℓ and $(\ell - r)/\ell$ (each with multiplicity ℓ), and its endomorphism algebra is $\mathbb{Q}(u) = L$.

We check that B is even absolutely simple. Consider $B_{\mathbb{F}_{p^e}}$ with $e \geq 1$. This is \mathbb{F}_{p^e} -isotypic since B is \mathbb{F}_p -simple, so the center of its endomorphism algebra is $\mathbb{Q}(u^e)$ with $u^e = \text{Fr}_{B_{\mathbb{F}_{p^e}}, p^e}$. To prove absolute simplicity we may replace e with a multiple so that $\ell|e$: $e = \ell e'$ for some $e' \in \mathbb{Z}$. Since $u^e = \alpha^{re'} \bar{\alpha}^{(\ell-r)e'}$ in \mathcal{O}_F generates the ideal $\wp^{re'} \bar{\wp}^{(\ell-r)e'}$ that does not come from \mathbb{Z} (due to the unequal exponents), the inclusion $\mathbb{Q}(u^e) \subseteq \mathbb{Q}(u^\ell) = F$ is an equality for degree reasons. Hence, if X is the unique (up to isogeny) simple factor of $B_{\mathbb{F}_{p^e}}$ then the endomorphism

algebra of X is a central division algebra D over F . The local invariants of D at the p -adic places v of F are the slopes of $B_{\mathbb{F}_{p^e}}$, which are r/ℓ and $(\ell - r)/\ell$. These have denominator ℓ , and D is split at all places of F away from p , so $\sqrt{[D : F]} = \ell$. Thus, Honda–Tate theory gives $2 \cdot \dim(X) = [F : \mathbb{Q}] \sqrt{[D : F]} = 2\ell$, so $\dim(X) = \ell = \dim(B_{\mathbb{F}_{p^e}})$. This gives the required absolute simplicity. (The reader can check that if $\ell \nmid e$ then $\mathbb{Q}(u^e) = \mathbb{Q}(u) = L$ and that this is the endomorphism algebra of $B_{\mathbb{F}_{p^e}}$, as for $e = 1$.)

Let M be a Galois closure of L over F . This is generated over \mathbb{Q} by $L = \mathbb{Q}(u)$ and $\mathbb{Q}(\mu_\ell)$, and it is Galois over \mathbb{Q} because u and p/u are respective ℓ th roots of the \mathbb{Q} -conjugate elements $p^r \alpha^{\ell-2r}$ and $p^r \alpha^{\ell-2r}$ in F that generate F over \mathbb{Q} . Since $[L : \mathbb{Q}] = 2\ell$, so F is the unique quadratic subfield of L , it follows from the linear disjointness of F and $\mathbb{Q}(\mu_\ell)$ over \mathbb{Q} that L and $\mathbb{Q}(\mu_\ell)$ are linearly disjoint over \mathbb{Q} . Hence, $[M : L] = \ell - 1$ and $[M : \mathbb{Q}] = 2\ell(\ell - 1)$. Since p splits in F and is inert in $\mathbb{Q}(\mu_\ell)$, $F(\mu_\ell)/F$ is inert at both primes over p . But L/F is totally ramified at both places, so by degree-counting we see that the composite field M of degree $\ell(\ell - 1)$ over F has exactly two p -adic places, each with residual degree $\ell - 1$ over \mathbb{F}_p . In particular, complex conjugation on the CM field M switches the two p -adic places of M and both such places are inert over L .

In addition to the preceding arithmetic properties of F and L at p , we need to record some group-theoretic properties before we can show that B does not satisfy (NI). Let $\Gamma := \text{Gal}(M/\mathbb{Q})$, $G := \text{Gal}(M/F)$, $H := \text{Gal}(M/L) = \text{Gal}(L(\mu_\ell)/L) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$, and $N := \text{Gal}(M/F(\mu_\ell)) \simeq \mathbb{Z}/\ell\mathbb{Z}$, so $\#N = \ell$, $\#H = \ell - 1$, and $G = N \rtimes H \simeq (\mathbb{Z}/\ell\mathbb{Z}) \rtimes (\mathbb{Z}/\ell\mathbb{Z})^\times$ with $(\mathbb{Z}/\ell\mathbb{Z})^\times$ acting on the additive group $\mathbb{Z}/\ell\mathbb{Z}$ via its canonical multiplicative scaling action. The group G has the following properties.

- (i) Let ℓ' be a prime divisor of $\ell - 1$ and let P be the ℓ' -Sylow subgroup of H . The normalizer subgroup $N_G(P)$ of P in G is equal to H . (In particular, $gHg^{-1} = H$ for $g \in G$ if and only if $g \in H$.)
- (ii) The only proper subgroups H' of G such that $N \cdot H' = G$ are the conjugates of H .
- (iii) Any two distinct conjugates of H intersect trivially.
- (iv) For any conjugate H' of H , there are exactly two orbits for the left H' -action on G/H . One orbit consists of a single coset and H' operates freely on the other H' -orbit.
- (v) Let Σ be a subset of G/H with $1 < \#\Sigma < \ell - 1$ (i.e., Σ and its complement Σ^c are subsets of G/H with more than one element). The subgroup $\text{Stab}_G(\Sigma) \subseteq G$ has image in $G/N = \text{Gal}(F(\mu_\ell)/F) = (\mathbb{Z}/\ell\mathbb{Z})^\times$ that is a proper subgroup of G/N .

The statement (i) is an easy calculation, the statements (ii) and (iii) follow from (i). (Statements (i)–(iii) are also easily seen in field-theoretic terms via the Galois correspondence.) The statement (iv) follows from (iii) (or is a simple calculation for $H' = H$, and for a general $H' = gHg^{-1}$ it follows from the fact that left multiplication by g^{-1} on G/H carries H' -orbits to H -orbits). Finally, (v) follows from (ii) and (iv) because if $\text{Stab}_G(\Sigma)$ maps onto G/N then by (ii) either $\text{Stab}_G(\Sigma) = G$ or $\text{Stab}_G(\Sigma)$ is a conjugate of H ; the first option contradicts that Σ is a proper subset of G/H and (by (iv)) the second option contradicts the assumptions on $\#\Sigma$.

Let Φ be a CM type of L that is a collection of embeddings of L into its Galois closure M over \mathbb{Q} . Such Φ 's are in bijective correspondence with H -invariant M -valued CM-types on M , which is to say subsets $\Phi_M \subseteq \Gamma$ satisfying $\Phi_M \cdot H = \Phi_M$ and $\Phi_M = \Psi \sqcup \iota \circ \Psi^c$, where ι

denotes the complex conjugation on the CM field M , $\Psi \subseteq G$, and Ψ^c is the complement of Ψ in G . (Here we have used that $\Gamma = G \times C$, where C is the subgroup generated by the central involution given by complex conjugation on the CM field M .) The H -stability condition on Φ_M says precisely that $\Psi \cdot H = \Psi$. If the above B over \mathbb{F}_p is to satisfy (NI) using a particular CM lift (over a normal local domain R with characteristic 0 and residue field \mathbb{F}_p , with R taken to be complete without loss of generality) then the Shimura–Taniyama formula in the residual reflex condition is exactly the requirement that the generic fiber of this lift has p -adic CM-type Φ on L corresponding to such a Φ_M with $\#(\Psi/H) = r$ or $\#(\Psi/H) = \ell - r$ (depending on which of the two p -adic places of M is induced by the choice of embedding of M into $\overline{\mathbb{Q}}_p$ so as to view M -valued CM-types on L or M as p -adic CM-types).

Hence, to prove that B does not satisfy (NI), it suffices to consider those M -valued Φ such that $1 < \#(\Psi/H) < \ell - 1$ (such Φ do exist) and to show that the second part of the residual reflex condition is violated at all p -adic places of the reflex field E of (L, Φ) . Since Ψ and Ψ^c have distinct cardinalities (as $r \neq \ell/2$) and complex conjugation is central in Γ , an element of Γ stabilizes $\Phi_M \subseteq \Gamma = \text{Gal}(M/\mathbb{Q})$ under the left action if and only if it stabilizes the non-empty subset $\Psi \subseteq G = \text{Gal}(M/F)$. In particular, $F \subseteq E$ due to the definition of E . Hence, in terms of Galois theory, the subfield $E \subseteq M$ corresponds to the subgroup $\text{Gal}(M/E) = \text{Stab}_G(\Psi/H)$ using the left G -action on $G/H = \text{Hom}_{\text{ring}}(L, M)$.

Since the reflex field E of (L, Φ) is a CM field (as is the reflex field of any CM type), complex conjugation acts nontrivially on this field. But complex conjugation on M switches the two p -adic places of M , and restriction to the imaginary quadratic field F in which p is split sets up a bijection between the p -adic places of M and of F . Thus, since $F \subseteq E$, we see that E admits exactly two p -adic places, these places are switched by complex conjugation on E , and each has decomposition group in $\text{Gal}(M/E)$ equal to the full Galois group. Since $M/F(\mu_\ell)$ is totally ramified at both p -adic places whereas $F(\mu_\ell)/F$ is unramified with full residual degree $\ell - 1$ at both of its p -adic places (since p is inert in $\mathbb{Q}(\mu_\ell)$ and split in F), the natural map from $\text{Gal}(M/E)$ to $G/N = \text{Gal}(F(\mu_\ell)/F)$ has image equal to the Galois group for the residue field extension for M/E at both p -adic places. Hence, the two p -adic places of E have residue field strictly larger than \mathbb{F}_p if and only if $\text{Gal}(M/E)$ has proper image in G/N . But $\text{Gal}(M/E) = \text{Stab}_G(\Psi/H)$, so property (v) above (applied to $\Sigma = \Psi/H \subseteq G/H$) implies that the p -adic places of E do indeed have nontrivial residual degree over \mathbb{F}_p . Thus, we have contradicted the second part of the residual reflex condition for the abelian variety B over \mathbb{F}_p , so it does not satisfy the property (NI).

To summarize, in these absolutely simple counterexamples to (NI) the endomorphism algebra over the finite field \mathbb{F}_p is a CM field L , but its CM-types that satisfy the requirement from the Shimura–Taniyama formula for a possible CM-lifting (over a complete local noetherian domain as in (I)) do not satisfy the second part of the residual reflex condition. Moreover, since \mathcal{O}_L has residue field \mathbb{F}_p at all p -adic places, by Proposition 2.1 these examples all satisfy (CML) and hence (I) over \mathbb{F}_p .

(3.6) Denote by \mathcal{NP}_{NI} (resp. $\mathcal{NP}_{p,\text{NI}}$) the set of all symmetric Newton polygons \mathfrak{N} such that every *isotypic* abelian variety B over a finite field \mathbb{F}_q (resp. over any finite field \mathbb{F}_q of characteristic p) with Newton polygon \mathfrak{N} satisfies (NI). If $\dim(B) = g > 0$ then this concave-up polygon is a concatenation of $2g$ segments whose slopes are the slopes of B (in the sense defined in §1.4, using suitably normalized p -adic ordinals of the roots of the characteristic polynomial of the q -Frobenius of B); these slopes lie in $\mathbb{Q} \cap [0, 1]$. The “symmetry” condition means that for every slope λ that occurs in \mathfrak{N} , the slopes λ and $1 - \lambda$ occur in \mathfrak{N} with the same

multiplicity, and the Newton polygons arising from abelian varieties are necessarily symmetric. For any symmetric Newton polygons $\mathfrak{N}_1, \dots, \mathfrak{N}_r$ with no slopes in common and non-negative integers m_1, \dots, m_r , we write $\sum m_j \mathfrak{N}_j$ to denote the symmetric Newton polygon obtained by concatenation of the segments in m_j copies of each \mathfrak{N}_j (with all segments arranged in order of increasing slope).

For each $n > 2$, let $(\frac{1}{n}, \frac{n-1}{n})$ denote the symmetric Newton polygon of length $2n$ with slopes $\frac{1}{n}$ and $\frac{n-1}{n}$ each occurring with multiplicity n . Analogously, we let $(\frac{1}{2}, \frac{1}{2})$ denote the symmetric Newton polygon with slope $\frac{1}{2}$ occurring with multiplicity 2, and we let $(0, 1)$ denote the symmetric Newton polygon with slopes 0 and 1 each occurring with multiplicity 1. We have seen examples of symmetric Newton polygons that are not in \mathcal{NP}_{NI} , namely $2(\frac{1}{2}, \frac{1}{2})$ and $(\frac{r}{\ell}, \frac{\ell-r}{\ell})$ for any odd prime $\ell \geq 5$ and $1 < r < \ell/2$. (In each case, the counterexamples were found in any characteristic $p > 0$ such that p satisfies a suitable non-vacuous congruence condition.) In the affirmative direction, the following are examples of symmetric Newton polygons \mathfrak{N} in \mathcal{NP}_{NI} .

- (i) An ordinary symmetric Newton polygon $\mathfrak{N} = g(0, 1)$, which is to say one whose only slopes (each with multiplicity $g > 0$) are 0 and 1, is in \mathcal{NP}_{NI} . This is exactly the case when the abelian variety B over a finite field k has p -divisible group with étale part having the maximal possible height, namely $g = \dim(B)$, or in other words B is an ordinary abelian variety. To establish (NI) for any such B , choose a CM subfield $L \subseteq \text{End}^0(B)$ with $[L : \mathbb{Q}] = 2g$ and pass to a k -isogenous abelian variety if necessary so that $\mathcal{O}_L \subseteq \text{End}(B)$. By the Serre–Tate deformation theorem [15, 1.2.1], to infinitesimally deform B with its \mathcal{O}_L -action is equivalent to doing the same for $B[p^\infty]$ with its \mathcal{O}_L -action. Upon choosing an \mathcal{O}_L -linear polarization λ of B over k (as we may do, by Lemma 2.2), the functoriality and uniqueness of deformations of étale and multiplicative p -divisible groups provide an \mathcal{O}_L -linear deformation Γ of $B[p^\infty]$ over $W(k)$ and an \mathcal{O}_L -linear $W(k)$ -isogeny $\Gamma \rightarrow \Gamma^t$ lifting the one induced by λ over k (where \mathcal{O}_L acts on $B[p^\infty]^t$ through the composition of Cartier duality and complex conjugation on \mathcal{O}_L). By the Serre–Tate theorem this corresponds to a formal abelian scheme \mathfrak{B} over $W(k)$ equipped with an \mathcal{O}_L -action and isogeny $\mathfrak{B} \rightarrow \mathfrak{B}^t$ that respectively lift the \mathcal{O}_L -action and polarization λ on B . Thus, by Grothendieck’s algebraization theorem, B satisfies (NI).
- (ii) The Newton polygon $(\frac{1}{2}, \frac{1}{2})$ corresponds to a supersingular elliptic curve E over a finite field k , and these satisfy (NI). (The counterexample to (NI) in §3.1 has Newton polygon $2(\frac{1}{2}, \frac{1}{2})$.) To prove this, choose an imaginary quadratic field $L \subseteq \text{End}^0(E)$ and pass to a k -isogenous elliptic curve if necessary so that $\mathcal{O}_L \subseteq \text{End}(E)$. Since $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_L$ acts on the 1-dimensional $E[p^\infty]$, by supersingularity there is a unique prime \mathfrak{p} in \mathcal{O}_L over p . Also, the action by \mathcal{O}_L on the tangent space to E defines an embedding of $\kappa = \mathcal{O}_L/\mathfrak{p}$ into k . Using this embedding to make k into an $\mathcal{O}_{L,\mathfrak{p}}$ -algebra, $E[p^\infty]$ corresponds to a 1-dimensional formal $\mathcal{O}_{L,\mathfrak{p}}$ -module G over k , and it has $\mathcal{O}_{L,\mathfrak{p}}$ -height 1 (since the \mathbb{Z}_p -height is 2 and $\mathcal{O}_{L,\mathfrak{p}}$ is finite free of rank 2 over \mathbb{Z}_p). Clearly $R = \mathcal{O}_{L,\mathfrak{p}} \otimes_{W(\kappa)} W(k)$ is a p -adic integer ring unramified over $\mathcal{O}_{L,\mathfrak{p}}$ with residue field k . Since elliptic curves are canonically projective, to lift E with its \mathcal{O}_L -action to R (having tangential action via $\mathcal{O}_{L,\mathfrak{p}} \hookrightarrow R$), it is equivalent to lift G to a formal $\mathcal{O}_{L,\mathfrak{p}}$ -module over R . By Lubin–Tate theory (or more generally the deformation theory of formal modules with finite height over algebras over p -adic integer rings [12, 22.4.4]), for any p -adic integer ring C and complete local noetherian C -algebra A , a height-1 formal C -module with dimension 1 over the residue field over A admits (up to unique isomorphism) a unique deformation

to a formal C -module over A . This provides the required lift of G over R as a formal $\mathcal{O}_{L,p}$ -module.

- (iii) Every Newton polygon of the form $\mathfrak{N} = (\frac{1}{n}, \frac{n-1}{n})$, $n > 2$, is in \mathcal{NP}_{NI} . Indeed, let B be an abelian variety over a finite field k (with size q) such that it has this Newton polygon; in particular, $\dim(B) = n$. Let $L \subseteq \text{End}^0(B)$ be a CM subfield with $[L : \mathbb{Q}] = 2n$, and use a k -isogeny if necessary so that $\mathcal{O}_L \subseteq \text{End}(B)$. The Frobenius element $\text{Fr}_{B,q} \in \mathcal{O}_L$ has p -adic slopes $\text{ord}_w(\text{Fr}_{B,q})/\text{ord}_w(q)$ given by only $1/n$ and $(n-1)/n = 1 - 1/n$. These are positive, so $G = B[p^\infty]$ is a connected p -divisible group with connected dual. If w is a p -adic place of L with associated slope $\lambda_w = \text{ord}_w(\text{Fr}_{B,q})/\text{ord}_w(q)$ then $\lambda_{\bar{w}} = 1 - \lambda_w \neq \lambda_w$, so $\bar{w} \neq w$. The faithful action of $\mathcal{O}_{L,p} \simeq \prod_{w|p} \mathcal{O}_{L,w}$ decomposes G into a product $\prod G_w$ where G_w is a nonzero connected p -divisible group equipped with an action by $\mathcal{O}_{L,w}$. The Dieudonné module $\mathbb{D}(G_w)$ is a nonzero flat module over $W(k) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L,w}$, and the action does not factor through a nontrivial factor ring because $\mathbb{D}(G_w)$ has an injective $\mathcal{O}_{L,w}$ -semilinear endomorphism that is semilinear over the absolute Frobenius automorphism of $W(k)$. Hence, G_w has height at least $[L_w : \mathbb{Q}_p]$, so since G has height $2n = [L : \mathbb{Q}]$ we see that G_w has height $[L_w : \mathbb{Q}_p]$.

Tate's method of proof of the Shimura–Taniyama formula in [29, §5] via p -divisible groups carries over to each G_w over the finite field k to yield the formula

$$\frac{\text{ord}_w(\text{Fr}_{B,q})}{\text{ord}_w(q)} = \frac{\dim(G_w)}{\text{height}(G_w)} = \frac{\dim(G_w)}{[L_w : \mathbb{Q}_p]}.$$

But the left side is either $1/n$ or $1 - 1/n$, and hence has denominator n . This forces $n|[L_w : \mathbb{Q}_p]$ for all w , yet $[L : \mathbb{Q}] = 2n$. Hence, there are exactly two p -adic places on L , necessarily of the form v and \bar{v} , say with respective slopes $1/n$ and $1 - 1/n > 1/n$. We also get $\dim(G_v) = 1$ and $\dim(G_{\bar{v}}) = n - 1$. The tangential action by $\mathcal{O}_{L,v}$ on the 1-dimensional G_v thereby defines an embedding $\kappa_v \hookrightarrow k$, and so G_v may be identified with a 1-dimensional formal $\mathcal{O}_{L,v}$ -module with $\mathcal{O}_{L,v}$ -height 1 over the $\mathcal{O}_{L,v}$ -algebra k . Applying the same considerations to the dual abelian variety B^t over k (with the usual dual CM-structure), we see that via the canonical isomorphism $\mathcal{O}_{L,v} \simeq \mathcal{O}_{L,\bar{v}}$ induced by complex conjugation, $G_{\bar{v}}$ is identified with the Cartier dual of a 1-dimensional formal $\mathcal{O}_{L,v}$ -module G'_v with $\mathcal{O}_{L,v}$ -height 1 over k .

Let $R = \mathcal{O}_{L,v} \otimes_{W(\kappa_v)} W(k)$, a p -adic integer ring unramified over $\mathcal{O}_{L,v}$ with residue field k . Using Lemma 2.2, choose an \mathcal{O}_L -linear polarization $\lambda : B \rightarrow B^t$. The associated map on p -divisible groups $G_v \times (G'_v)^t \rightarrow G'_v \times (G_v)^t$ decomposes as the product $\lambda_v \times \mu_v^t$ of an $\mathcal{O}_{L,v}$ -linear isogeny $\lambda_v : G_v \rightarrow G'_v$ and the dual of another such isogeny $\mu_v : G_v \rightarrow G'_v$. To prove (NI) for B , it suffices to deform λ_v and μ_v over R ; we handle λ_v , and then μ_v will go in the same way. Arguing via deformation theory of 1-dimensional formal C -modules of C -height 1 over complete local noetherian algebras over p -adic integer rings C , exactly as in (ii) we may uniquely deform G_v and G'_v over R . There is at most one lift of λ_v , and so if \bar{k}/k is an algebraic closure then by Galois theory (adapted to the completed maximal unramified extension $W(k) \rightarrow W(\bar{k})$) it suffices to construct such a lift when k is replaced with \bar{k} . But G_v and G'_v become $\mathcal{O}_{L,v}$ -linearly isomorphic over \bar{k} , so λ_v becomes multiplication by some nonzero element of $\mathcal{O}_{L,v}$. Uniqueness of deformations in the height-1 case thereby settles the lifting problem for λ_v .

It is easy to adapt the arguments underlying the preceding examples (i)–(iii) to show that

any symmetric Newton polygon that can be written as a finite sum in the form

$$\mathfrak{N} = m_1(0, 1) + \sum_{n \geq 2} m_n \left(\frac{1}{n}, \frac{n-1}{n} \right), \quad m_1 \geq 0, m_n \in \{0, 1\} \text{ for all } n \geq 2,$$

is in \mathcal{NP}_{NI} . We do not know whether there is an element of \mathcal{NP}_{NI} that is not of the above form.

(3.7) Remark (i) The method of using Galois extensions whose Galois group is the standard semi-direct product $G \simeq (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ fails dramatically when $n = 15$. In this case we have $N \simeq \mathbb{Z}/15\mathbb{Z}$ and $H = (\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$. The left action of H on G/H is identified with the standard action of $(\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$ on $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$, and this has 4 orbits (namely, $\{0\}$, $(\mathbb{Z}/3\mathbb{Z})^\times$, $(\mathbb{Z}/5\mathbb{Z})^\times$, and the rest) with respective cardinalities 1, 2, 4, and 8. Therefore, for any integer r with $1 \leq r \leq 14$ there exists a subset of G/H with r elements that is stable under the left action by H , and so likewise for the left action on G/H by any conjugate of H .

(ii) It would be interesting to determine which symmetric Newton polygons belong to \mathcal{NP}_{NI} , and which ones belong to $\mathcal{NP}_{p,\text{NI}}$ as the prime number p varies. For a given symmetric Newton polygon \mathfrak{N} , the question as to whether \mathfrak{N} belongs to $\mathcal{NP}_{p,\text{NI}}$ is easier when p does not divide the denominator of any slope of \mathfrak{N} . For instance it is not difficult to check that $(\frac{r}{15}, \frac{15-r}{15})$ is in $\mathcal{NP}_{p,\text{NI}}$ for $r = 2, 4, 6, 7$ if $p \neq 3, 5$. We do not know any plausible statistics about \mathcal{NP}_{NI} or $\mathcal{NP}_{p,\text{NI}}$ among all symmetric Newton polygons.

§4. Algebraic Hecke characters

In this section we will first review the definition and basic properties of algebraic Hecke characters before establishing Theorem 4.11, which gives a procedure to modify an algebraic Hecke character. The reader is referred to [30], [25, §7], [24, Chap. II], [7, §5], [20], and [19] for more information about algebraic Hecke characters. We sometimes write \underline{L}^\times as shorthand for the algebraic group $\text{Res}_{L/\mathbb{Q}}(\mathbb{G}_m)$ over \mathbb{Q} , where $\text{Res}_{L/\mathbb{Q}}$ denotes Weil restriction with respect to a finite extension L/\mathbb{Q} .

(4.1) Definition Let k be an infinite field. For a finite separable extension F/k and an extension K/k , a homomorphism $\chi : F^\times \rightarrow K^\times$ is *algebraic* (with respect to k) if one of the following equivalent conditions holds:

- (i) The map χ is induced by a homomorphism

$$\text{Res}_{F/k}(\mathbb{G}_m) \otimes_k K \xrightarrow{\phi} \mathbb{G}_m$$

of algebraic groups over K . The relation between χ and ϕ is that the map $(F \otimes_k K)^\times \rightarrow K^\times$ induced by ϕ on K -points restricts to χ on the subgroup $F^\times \subseteq (F \otimes_k K)^\times$ (inclusion defined by $t \mapsto t \otimes 1$).

- (ii) (K/k finite separable) The map χ is induced by a k -homomorphism

$$\text{Res}_{F/k}(\mathbb{G}_m) \rightarrow \text{Res}_{K/k}(\mathbb{G}_m).$$

- (iii) Let e_1, \dots, e_n be a k -basis of F . Then there exists a rational function $f(X_1, \dots, X_n) \in K(X_1, \dots, X_n)$ such that every non-zero element of k^n is in the domain of definition of $f(X_1, \dots, X_n)$ and

$$\chi \left(\sum_{i=1}^n x_i e_i \right) = f(x_1, \dots, x_n)$$

for every non-zero element $(x_1, \dots, x_n) \in k^n$.

- (iv) Let $I = \text{Hom}_{\text{ring}}(F, K_s)$ be the finite set of embeddings of F into a (fixed) separable closure K_s of K . Then there exists a $\text{Gal}(K_s/K)$ -invariant function $m : I \rightarrow \mathbb{Z}$, necessarily unique, such that

$$\chi(x) = \prod_{\tau \in I} \tau(x)^{m(\tau)}$$

for all $x \in F^\times$.

The equivalence of (i) and (ii) is due to functorial adjointness, and the equivalence of (i) and (iv) is clear, as is the implication (iv) \Rightarrow (iii). Finally, to deduce (i) from (iii) one uses that the set of k -points is Zariski-dense in any torus over k (such as $\text{Res}_{F/k}(\mathbb{G}_m)$) and that a rational map between algebraic groups over a field is a morphism if it is generically a homomorphism (in an evident sense).

(4.2) Remark In practice the ground field k is understood from context (for us it will be \mathbb{Q} , except in §6 where we sometimes use $k = \mathbb{Q}_p$). The Galois group $\text{Gal}(K_s/K)$ operates naturally on I in condition (iv). The displayed equation in (iv) implies that m is constant on each $\text{Gal}(K_s/K)$ -orbit of I . Conversely, for any function $m : I \rightarrow \mathbb{Z}$ which is constant on every $\text{Gal}(K_s/K)$ -orbit of I there is a unique algebraic homomorphism χ from F^\times to K^\times giving rise to m as in (iv). If $K \subseteq F$ (over k) then the special case with m identically equal to 1 corresponds to $\chi = \text{Nm}_{F/K}$. If K/k splits F/k then $\text{Gal}(K_s/K)$ acts trivially on I , so in such cases the maps $F^\times \rightarrow K^\times$ induced by field embeddings are a \mathbb{Z} -basis for the group of algebraic homomorphisms (with respect to k).

(4.3) Definition Let F be a number field. Let \mathfrak{m} be a nonzero ideal of the ring of integers \mathcal{O}_F of F . Let $I_{\mathfrak{m}}$ be the group of fractional ideals of \mathcal{O}_F that are relatively prime to \mathfrak{m} . Let \mathbb{A}_F^\times be the group of F -ideles. Let K be a field of characteristic 0.

- (a) A homomorphism $\chi : I_{\mathfrak{m}} \rightarrow K^\times$ is an *algebraic Hecke character with conductor \mathfrak{m}* if there exists a homomorphism $\chi_{\text{alg}} : F^\times \rightarrow K^\times$ that is algebraic (with respect to \mathbb{Q}) such that

$$\chi((x)) = \chi_{\text{alg}}(x)$$

for every $x \in F^\times$ satisfying two conditions: $x \equiv 1 \pmod{\mathfrak{m}}$ and x has image in F_∞^\times lying in the identity component $(F_\infty^\times)^0$ (i.e., x is positive at all real places). Here, $(x) = x\mathcal{O}_F$ is the principal fractional ideal of \mathcal{O}_F generated by x .

- (b) A continuous homomorphism $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ is an *algebraic Hecke character* if there exists an algebraic homomorphism $\epsilon_{\text{alg}} : F^\times \rightarrow K^\times$ (with respect to \mathbb{Q}) such that the restriction $\epsilon|_{F^\times}$ of ϵ to the diagonally embedded subgroup $F^\times \subseteq \mathbb{A}_F^\times$ is equal to ϵ_{alg} . Here, the target K^\times of ϵ is given the discrete topology, so the kernel of ϵ is an open subgroup of \mathbb{A}_F^\times .

The equivalence of the two definitions can be seen as follows. Suppose that $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ is an algebraic Hecke character as in (b) above. Choose a nonzero ideal \mathfrak{m} of \mathcal{O}_F such that $\ker(\epsilon)$ contains the open subgroup

$$U_{\mathfrak{m}} := (F_\infty^\times)^0 \times \prod_{v|\mathfrak{m}} (1 + \mathfrak{m}\mathcal{O}_{F,v}) \times \prod_{v \notin S} \mathcal{O}_{F,v}^\times$$

of \mathbb{A}_F^\times , where $S = S(\mathfrak{m})$ is the union of the archimedean places of F and the set of places of F dividing \mathfrak{m} . Denote by \mathbb{A}_F^S the factor ring of \mathbb{A}_F consisting of factors away from S (i.e., the restricted product $\prod'_{v \notin S} F_v$), so its unit group is the restricted product $\mathbb{A}_F^{S,\times} = \prod'_{v \notin S} F_v^\times$. The restriction $\epsilon|_{\mathbb{A}_F^{S,\times}}$ of ϵ to $\mathbb{A}_F^{S,\times}$ factors through the canonical surjection $\pi_S : \mathbb{A}_F^{S,\times} \twoheadrightarrow I_{\mathfrak{m}}$ and gives a homomorphism $\chi : I_{\mathfrak{m}} \rightarrow K^\times$ satisfying the conditions in (a). Both χ and ϵ are said to have conductor $\leq \mathfrak{m}$.

Conversely, given a homomorphism $\chi : I_{\mathfrak{m}} \rightarrow K^\times$ satisfying the conditions in (a), one defines a continuous homomorphism $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ as follows. Every element $x \in \mathbb{A}_F^\times$ can be written as a product $x = u \cdot y \cdot z$ with $u \in U_{\mathfrak{m}}$, $y \in F^\times$, and $z \in \mathbb{A}_F^{S,\times}$, where S is as in the previous paragraph. Define $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ by $\epsilon(x) = \chi_{\text{alg}}(y)\chi(\pi_S(z))$ for $x = uyz$ as above. It is easy to see that ϵ is well-defined and satisfies the conditions in (b). Note that if χ and ϵ correspond to each other as above, then the algebraic homomorphisms χ_{alg} and ϵ_{alg} are equal; this algebraic homomorphism is called the *algebraic part* of χ or ϵ . As an example, if F'/F is a finite extension and \mathfrak{m}' is a sufficiently divisible modulus on F' lying over \mathfrak{m} such that $\mathfrak{m}|\text{Nm}(\mathfrak{m}')$, then $\epsilon \circ \text{Nm}_{F'/F}$ is an algebraic Hecke character with algebraic part $\epsilon_{\text{alg}} \circ \text{Nm}_{F'/F}$ and associated homomorphism $I_{\mathfrak{m}'} \rightarrow K^\times$ given by $\chi \circ \text{Nm}_{F'/F}$.

Note that the concepts of algebraic character and algebraic Hecke character as discussed above make sense when $K = \prod K_i$ is a finite product of fields K_i of characteristic 0, an interesting example of which is $L_\ell := \mathbb{Q}_\ell \otimes_{\mathbb{Q}} L$ for a number field L . In such cases, the preceding assertions (and their proofs) concerning algebraic characters and algebraic Hecke characters carry over essentially verbatim, and these properties hold if and only if they do after composing with projection to each factor field K_i .

(4.4) The concept of algebraic Hecke character can be expressed in terms of (possibly disconnected) linear algebraic \mathbb{Q} -groups $S_{\mathfrak{m}}$ defined in Chapter II of [24]. This will be very useful for our purposes, so we now recall the definition of $S_{\mathfrak{m}}$ and use it to formulate a bijective correspondence between K^\times -valued algebraic Hecke characters of a number field F and certain continuous representations $\text{Gal}(F^{\text{ab}}/F) \rightarrow K_\ell^\times$ for any number field K (and a fixed rational prime ℓ).

The group $S_{\mathfrak{m}}$ is an extension of the finite group $C_{\mathfrak{m}} := \mathbb{A}_F^\times / (F^\times \cdot U_{\mathfrak{m}})$ by a certain \mathbb{Q} -torus $T_{\mathfrak{m}}$. By definition, $T_{\mathfrak{m}}$ is the quotient of $\underline{F}^\times := \text{Res}_{F/\mathbb{Q}}(\mathbb{G}_m)$ by the Zariski closure of the image of the finitely generated \mathbb{Z} -module $F^\times \cap U_{\mathfrak{m}}$ in \underline{F}^\times . The \mathbb{Q} -torus $T_{\mathfrak{m}}$ stabilizes as a quotient of \underline{F}^\times when \mathfrak{m} is sufficiently divisible (since the closure of $F^\times \cap U_{\mathfrak{m}}$ in \underline{F}^\times has identity component that is independent of \mathfrak{m}); we denote it by \mathfrak{S}^F , following the notation in [19]. Note that the notation for the \mathbb{Q} -torus \mathfrak{S}^F is S^F in [20] and is ${}^F S$ in [8]. By definition, the extension

$$1 \rightarrow T_{\mathfrak{m}} \rightarrow S_{\mathfrak{m}} \rightarrow C_{\mathfrak{m}} \rightarrow 1$$

which defines $S_{\mathfrak{m}}$ is the push-out of the short exact sequence

$$1 \rightarrow F^\times / (F^\times \cap U_{\mathfrak{m}}) \rightarrow \mathbb{A}_F^\times / U_{\mathfrak{m}} \rightarrow C_{\mathfrak{m}} \rightarrow 1$$

by the natural homomorphism $F^\times/(F^\times \cap U_{\mathfrak{m}}) \rightarrow T_{\mathfrak{m}}(\mathbb{Q})$. In other words, we have a commutative diagram of locally finite type \mathbb{Q} -groups

$$\begin{array}{ccccccc} 1 & \longrightarrow & F^\times/F^\times \cap U_{\mathfrak{m}} & \longrightarrow & \mathbb{A}_F^\times/U_{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} \longrightarrow 1 \\ & & \downarrow & & \downarrow i_{F,\mathfrak{m}} & & \downarrow = \\ 1 & \longrightarrow & T_{\mathfrak{m}} & \longrightarrow & S_{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} \longrightarrow 1, \end{array}$$

with exact rows (and the top row consisting of constant groups). In particular, $i_{F,\mathfrak{m}}$ can equivalently be viewed as a map of abstract groups $\mathbb{A}_F^\times/U_{\mathfrak{m}} \rightarrow S_{\mathfrak{m}}(\mathbb{Q})$, and its image is Zariski-dense in $S_{\mathfrak{m}}$. These commutative diagrams form a projective system as \mathfrak{m} runs through all nonzero ideals of \mathcal{O}_F .

Taking the inverse limit of the short exact sequences

$$1 \rightarrow T_{\mathfrak{m}} \rightarrow S_{\mathfrak{m}} \rightarrow C_{\mathfrak{m}} \rightarrow 1$$

over nonzero ideals \mathfrak{m} of \mathcal{O}_F , we get an exact sequence

$$1 \rightarrow \mathfrak{S}^F \rightarrow S_F \rightarrow \text{Gal}(F^{\text{ab}}/F) \rightarrow 1$$

of proalgebraic groups over \mathbb{Q} ; this exact sequence is the pullback of the exact sequence $1 \rightarrow T_{\mathfrak{m}} \rightarrow S_{\mathfrak{m}} \rightarrow C_{\mathfrak{m}} \rightarrow 1$ by the canonical surjection $\text{Gal}(F^{\text{ab}}/F) \rightarrow C_{\mathfrak{m}}$ for \mathfrak{m} sufficiently divisible so that $T_{\mathfrak{m}}$ does not change (as a quotient of \underline{F}^\times) when \mathfrak{m} is replaced with any nonzero multiple. Here we have used class field theory to identify $\varprojlim C_{\mathfrak{m}}$ with $\text{Gal}(F^{\text{ab}}/F)$ as profinite groups. Note that we have a natural commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & F^\times & \longrightarrow & \mathbb{A}_F^\times & \longrightarrow & \mathbb{A}_F^\times/F^\times \longrightarrow 1 \\ & & \downarrow & & \downarrow i_F & & \downarrow \text{rec}_F \\ 1 & \longrightarrow & \mathfrak{S}^F(\mathbb{Q}) & \longrightarrow & S_F(\mathbb{Q}) & \longrightarrow & \text{Gal}(F^{\text{ab}}/F) \longrightarrow 1 \end{array}$$

where $\text{rec}_F : \mathbb{A}_F^\times/F^\times \rightarrow \text{Gal}(F^{\text{ab}}/F)$ is the Artin map with the classical (arithmetic) normalization.

By definition of the proalgebraic group structure on S_F , any \mathbb{Q} -rational homomorphism from S_F to a finite type algebraic group over \mathbb{Q} factors through the projection to some $S_{\mathfrak{m}}$. The following lemma gives another description of algebraic Hecke characters of F . The proof is omitted. (See §2.6 in Chapter II of [24].)

(4.5) Lemma *Let K be a number field.*

- (i) *Let $\rho : S_F \rightarrow \underline{K}^\times$ (resp. $\rho_{\mathfrak{m}} : S_{\mathfrak{m}} \rightarrow \underline{K}^\times$) be a \mathbb{Q} -rational homomorphism. The composition*

$$\mathbb{A}_F^\times \xrightarrow{i_F} S_F(\mathbb{Q}) \xrightarrow{\rho} \underline{K}^\times(\mathbb{Q}) = K^\times$$

is an algebraic Hecke character (resp. the composition

$$I_{\mathfrak{m}} = \mathbb{A}_F^{S(\mathfrak{m}),\times} / \prod_{v \notin S(\mathfrak{m})} \mathcal{O}_{F,v}^\times \longrightarrow \mathbb{A}_F^\times/U_{\mathfrak{m}} \xrightarrow{i_{F,\mathfrak{m}}} S_{\mathfrak{m}}(\mathbb{Q}) \xrightarrow{\rho_{\mathfrak{m}}} \underline{K}^\times(\mathbb{Q}) = K^\times$$

is an algebraic Hecke character with conductor $\leq \mathfrak{m}$).

- (ii) *Conversely, every algebraic Hecke character $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ (resp. algebraic Hecke character $\chi : I_{\mathfrak{m}} \rightarrow K^\times$ with conductor $\leq \mathfrak{m}$) comes from a unique \mathbb{Q} -rational homomorphism $\rho : S_F \rightarrow \underline{K}^\times$ (resp. $\rho_{\mathfrak{m}} : S_{\mathfrak{m}} \rightarrow \underline{K}^\times$).*

(4.6) Remark (i) In the situation of Lemma 4.5, the composition of the quotient map $\underline{F}^\times \rightarrow \mathfrak{S}^F$ with the restriction $\rho|_{\mathfrak{S}^F}$ of ρ to $\mathfrak{S}^F \subseteq S^F$ is the algebraic part ϵ_{alg} of the algebraic Hecke character ϵ .

(ii) For later reference, we record the following fact: any two algebraic Hecke characters $\epsilon_1, \epsilon_2 : \mathbb{A}_F^\times \rightarrow K^\times$ with the same algebraic part coincide on an open subgroup of finite index containing F^\times . This is easily seen from any of the equivalent definitions of the concept of algebraic Hecke character.

(4.7) When the extension $1 \rightarrow \mathfrak{S}^F \rightarrow S_F \rightarrow \text{Gal}(F^{\text{ab}}/F) \rightarrow 1$ of proalgebraic groups over \mathbb{Q} is viewed over the \mathbb{Q} -algebra \mathbb{A}_f , it admits a natural continuous splitting $\phi : \text{Gal}(F^{\text{ab}}/F) \rightarrow S_F(\mathbb{A}_f) = \varprojlim S_{\mathfrak{m}}(\mathbb{A}_f)$ over the subgroup of “constant points” in the constant proalgebraic group scheme $\text{Gal}(F^{\text{ab}}/F)$ over $\text{Spec}(\mathbb{A}_f)$. We review its construction below; in Chapter II, §2.3 in [24] the associated continuous ℓ -adic splittings $\phi_\ell : \text{Gal}(F^{\text{ab}}/F) \rightarrow S_F(\mathbb{Q}_\ell) = \varprojlim S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ over \mathbb{Q}_ℓ are constructed (or rather, the composite of this with projection to each $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is constructed and is denoted ε_ℓ with \mathfrak{m} fixed). The splitting ϕ does *not* extend to a splitting as proalgebraic group schemes over $\text{Spec}(\mathbb{A}_f)$, since a map from an affine proalgebraic group scheme to a finitely presented affine group scheme factors through an algebraic quotient of the source whereas the splitting maps $\text{Gal}(F^{\text{ab}}/F) \rightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ that we shall construct will not factor through any finite quotient $C_{\mathfrak{m}'}$ of the source.

To construct ϕ it suffices to construct a compatible family of continuous homomorphisms $\phi_{\mathfrak{m}} : \text{Gal}(F^{\text{ab}}/F) \rightarrow S_{\mathfrak{m}}(\mathbb{A}_f)$, where $\phi_{\mathfrak{m}}$ lifts the canonical quotient map $\text{Gal}(F^{\text{ab}}/F) \rightarrow C_{\mathfrak{m}}$ (whose target is viewed as \mathbb{Q} -points within the \mathbb{A}_f -points of the finite constant \mathbb{Q} -group associated to $C_{\mathfrak{m}}$). Let $\pi_{\mathfrak{m}} : \underline{F}^\times \rightarrow T_{\mathfrak{m}}$ be the canonical quotient map over \mathbb{Q} . Define $\tilde{\phi}_{\mathfrak{m}} : \mathbb{A}_F^\times \rightarrow S_{\mathfrak{m}}(\mathbb{A}_f)$ by

$$\tilde{\phi}_{\mathfrak{m}}(x) = i_{F,\mathfrak{m}}(x \bmod U_{\mathfrak{m}}) \cdot \pi_{\mathfrak{m}}(x_f)^{-1}.$$

Here, $x = (x_\infty, x_f)$ with $x_\infty \in F_\infty^\times$ and $x_f \in \mathbb{A}_{F,f}^\times$ denoting the archimedean and finite components of x respectively. The point $i_{F,\mathfrak{m}}(x) \in S_{\mathfrak{m}}(\mathbb{Q})$ is viewed as an element of $S_{\mathfrak{m}}(\mathbb{A}_f)$ in the natural manner, and $\pi_{\mathfrak{m}}(x_f) \in T_{\mathfrak{m}}(\mathbb{A}_f) \subseteq S_{\mathfrak{m}}(\mathbb{A}_f)$, so $i_{F,\mathfrak{m}}(x \bmod U_{\mathfrak{m}}) \cdot \pi_{\mathfrak{m}}(x_f)^{-1}$ makes sense as an element of $S_{\mathfrak{m}}(\mathbb{A}_f)$. By construction, the map $\tilde{\phi}_{\mathfrak{m}}$ is continuous and its restriction to F^\times is trivial. Thus, $\tilde{\phi}_{\mathfrak{m}}$ factors continuously through the projection $\mathbb{A}_F^\times \rightarrow \mathbb{A}_F^\times/F^\times$. Since the target group of $\tilde{\phi}_{\mathfrak{m}}$ is totally disconnected, $\tilde{\phi}_{\mathfrak{m}}$ factors through the topological quotient $\mathbb{A}_F^\times \rightarrow \pi_0(\mathbb{A}_F^\times/F^\times) \simeq \text{Gal}(F^{\text{ab}}/F)$ to define a continuous homomorphism $\phi_{\mathfrak{m}} : \text{Gal}(F^{\text{ab}}/F) \rightarrow S_{\mathfrak{m}}(\mathbb{A}_f)$. The compatibility with respect to change in \mathfrak{m} is easy to check. For every prime number ℓ , define the continuous map

$$\phi_\ell := \pi_\ell \circ \phi : \text{Gal}(F^{\text{ab}}/F) \rightarrow S_F(\mathbb{Q}_\ell),$$

where $\pi_\ell : S_F(\mathbb{A}_f) \rightarrow S_F(\mathbb{Q}_\ell)$ is the homomorphism induced by the projection $\mathbb{A}_f \rightarrow \mathbb{Q}_\ell$. The associated ℓ -adic splitting $\text{Gal}(F^{\text{ab}}/F) \rightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is the ℓ -adic component of $\phi_{\mathfrak{m}}$.

(4.8) Lemma *Let $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ be an algebraic Hecke character corresponding to a \mathbb{Q} -rational homomorphism $\rho : S_F \rightarrow \underline{K}^\times$, with K a number field. Let ℓ be a prime number. Then*

$$\psi_\ell := \rho \circ \phi_\ell : \text{Gal}(F^{\text{ab}}/F) \rightarrow \underline{K}^\times(\mathbb{Q}_\ell) = K_\ell^\times$$

is a continuous homomorphism with the following properties.

- (i) There exists a finite set S of places of F , including all archimedean places and all places above ℓ , such that ψ_ℓ is unramified outside S and $\psi_\ell(W_v) \subseteq K^\times$ for each place $v \notin S$ of F , where W_v is the Weil subgroup of the decomposition group of v in $\text{Gal}(F^{\text{ab}}/F)$. In fact, $\psi_\ell(\text{Frob}_v) = \epsilon(\pi_v)$, where π_v is any local uniformizer at $v \notin S$ and $\text{Frob}_v \in \text{Gal}(F^{\text{ab}}/F)$ is an arithmetic Frobenius element at v .
- (ii) The representation ψ_ℓ is locally algebraic above ℓ . In fact, the composition

$$\psi_\ell \circ \text{rec}_{F,\ell} : F_\ell^\times := \prod_{\lambda|\ell} F_\lambda^\times \rightarrow K_\ell^\times$$

of ψ_ℓ with the finite product of local Artin maps

$$\text{rec}_{F,\ell} : F_\ell^\times := \prod_{\lambda|\ell} F_\lambda^\times \rightarrow \prod_{\lambda|\ell} \text{Gal}(F_\lambda^{\text{ab}}/F_\lambda) \rightarrow \text{Gal}(F^{\text{ab}}/F)$$

coincides with the algebraic homomorphism

$$\epsilon_{\text{alg}}^{-1} : F_\ell^\times = \underline{F}^\times(\mathbb{Q}_\ell) \rightarrow \underline{K}^\times(\mathbb{Q}_\ell) = K_\ell^\times$$

on an open subgroup of F_ℓ^\times .

Moreover, if ρ factors canonically through a homomorphism $\rho_{\mathfrak{m}} : S_{\mathfrak{m}} \rightarrow \underline{K}^\times$ then $\psi_\ell = \rho_{\mathfrak{m}} \circ (\phi_{\mathfrak{m}})_\ell$, where $(\phi_{\mathfrak{m}})_\ell$ is the \mathbb{Q}_ℓ -part of $\phi_{\mathfrak{m}}$.

PROOF. The assertion in (i) is immediate from the definitions. Note that if ϵ has conductor $\leq \mathfrak{m}$, then the set S in (i) can be taken to be the union of the set of all archimedean places of F and the set of all places of F dividing \mathfrak{m} . (See also Chapter II, §2.5 in [24].) Also, the description of ψ_ℓ in terms of $\rho_{\mathfrak{m}}$ if ρ factors through $\rho_{\mathfrak{m}}$ is clear from the definitions.

As for (ii), first observe that for $x \in F^\times$ we have $\psi_\ell(\text{rec}_{F,\ell}(x)) = \psi_\ell(r_F((x)^{(\ell)}))^{-1}$ where $(x)^{(\ell)} \in \mathbb{A}_F^\times$ is the idele that is trivial at all $v|\ell$ and is given by x at all $v \nmid \ell$. But for any finite place $v \nmid \ell$ on F , the image of inertia at v in $\text{Gal}(F^{\text{ab}}/F)$ has finite pro- ℓ part, so since ψ_ℓ is mapping continuously into K_ℓ^\times we see that by taking x sufficiently near 1 at all $v \in S$ with $v \nmid \ell$ we have $\psi_\ell(r_F((x)^{(\ell)})) = \psi_\ell(r_F((x)^{(S)}))$ where $(x)^{(S)} \in \mathbb{A}_F^{S,\times}$ is the idele that is trivial at S and given by x at all places away from S . By (i), $\psi_\ell(r_F((x)^{(S)})) = \epsilon((x)^{(S)})$. Taking x to also satisfy $x \equiv 1 \pmod{\mathfrak{m}}$ where \mathfrak{m} is the modulus of ϵ , it follows from the algebraicity of ϵ that $\epsilon((x)^{(S)}) = \epsilon_{\text{alg}}(x)$ for such x . Hence, $\psi_\ell(\text{rec}_{F,\ell}(x)) = \epsilon_{\text{alg}}(x)^{-1}$ for $x \in F^\times$ that is sufficiently close to 1 at all $v \in S$. Using these nearness conditions at $v|\ell$ gives an open neighborhood V_ℓ of the identity in F_ℓ^\times on which the desired identity holds because it does so on the dense subset $F^\times \cap V_\ell$. \square

The following converse lemma includes a uniqueness result for ψ_ℓ as in Lemma 4.8, and it will be useful later when we need to check an equality of algebraic Hecke characters.

(4.9) Lemma *Let F and K be number fields. Let ℓ be a prime number, and let S be a finite set of places of F including all archimedean places and all places above ℓ . Let $\psi_\ell : \text{Gal}(F^{\text{ab}}/F) \rightarrow K_\ell^\times$ be a continuous homomorphism that is unramified outside S and for which $\psi_\ell(W_v) \subseteq K^\times$ for all Weil subgroups W_v in decomposition groups $D_v \subseteq \text{Gal}(F^{\text{ab}}/F)$ at $v \notin S$. Assume moreover that there exists a \mathbb{Q} -homomorphism $\chi_{\text{alg}} : \underline{F}^\times \rightarrow \underline{K}^\times$ such that $\psi_\ell \circ \text{rec}_{F,\ell}$ coincides*

with χ_{alg} on an open subgroup U_ℓ of $F_\ell^\times = \underline{F}^\times(\mathbb{Q}_\ell)$. There exists a unique algebraic Hecke character $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ whose algebraic part ϵ_{alg} is χ_{alg}^{-1} such that ϵ induces ψ_ℓ as in Lemma 4.8. In particular, if F'/F is a finite extension then $\epsilon \circ \text{Nm}_{F'/F}$ corresponds to $\psi_\ell|_{\text{Gal}(F'^{\text{ab}}/F')}$.

PROOF. Let $r_F : \mathbb{A}_F^\times \rightarrow \text{Gal}(F^{\text{ab}}/F)$ be the composition of $\mathbb{A}_F^\times \rightarrow \mathbb{A}_F^\times/F^\times$ with the Artin map $\text{rec}_F : \mathbb{A}_F^\times/F^\times \rightarrow \text{Gal}(F^{\text{ab}}/F)$. Define $\epsilon : \mathbb{A}_F^\times \rightarrow K_\ell^\times$ by

$$\epsilon(x) = \psi_\ell(r_F(x)) \cdot \chi_{\text{alg}}^{-1}(x_\ell), \quad (3)$$

where $x_\ell \in F_\ell^\times$ denotes the ℓ -adic component of $x \in \mathbb{A}_F^\times$. Choose an open subgroup W of $\prod_{p \in S, p \neq \ell, \infty} F_p^\times$ such that $(\psi_\ell \circ r_F)(W) = \{1\}$; such an open subgroup W exists because ψ_ℓ is continuous and takes values in a finite product of multiplicative groups of ℓ -adic fields. It is clear that ϵ is trivial on the open subgroup

$$U := (F_\infty^\times)^0 \times U_\ell \times W \times \prod_{v \notin S} \mathcal{O}_{F,v}^\times$$

of \mathbb{A}_F^\times . It is also clear that ϵ coincides with χ_{alg}^{-1} on F^\times . Since \mathbb{A}_F^\times is generated by U , F^\times and $(\mathbb{A}_F^S)^\times$, we have $\epsilon(\mathbb{A}_F^\times) \subseteq K^\times$. Thus, ϵ is an algebraic Hecke character with χ_{alg}^{-1} as its algebraic part. Moreover, ϵ is unramified away from S and $\psi_\ell(\text{Frob}_v) = \epsilon(\pi_v)$ for all $v \notin S$, so by continuity of ψ_ℓ we see that this ψ_ℓ is the same as the one arising from ϵ in Lemma 4.8.

As for the uniqueness of ϵ , it has to be proved that if ϵ is a K^\times -valued finite-order Hecke character of F with $\rho_\epsilon \circ \phi_\ell = 1$ (where $\rho_\epsilon : S_F \rightarrow \underline{K}^\times$ corresponds to ϵ) then $\epsilon = 1$. But $\epsilon(\pi_v) = 1$ for all but finitely many v , so the result follows. The final part concerning $\epsilon \circ \text{Nm}_{F'/F}$ follows from the uniqueness and the relationship in class field theory between Galois restriction and norm maps. \square

The next lemma will play a technical role in the proof of the main arithmetic result in this section, Theorem 4.11.

(4.10) Lemma *Let Γ_0 be a normal subgroup of finite index in a group Γ . Let γ be an element of Γ of infinite order, and let $\Gamma_1 := \Gamma_0 \cdot \gamma^\mathbb{Z}$ be the subgroup of Γ generated by Γ_0 and γ . Let n be the unique positive integer such that $\langle \gamma^n \rangle = \Gamma_0 \cap \gamma^\mathbb{Z}$. Let $\rho_0 : \Gamma_0 \rightarrow H$ be a homomorphism of groups. Let $h \in H$ be an element of H such that $h^n = \rho_0(\gamma^n)$. Assume that $\rho_0(\gamma x \gamma^{-1}) = h \rho_0(x) h^{-1}$ for all $x \in \Gamma_0$. Then there exists a unique extension of ρ_0 to a homomorphism*

$$\rho_1 : \Gamma_1 \rightarrow H$$

such that $\rho_1(\gamma) = h$.

PROOF. Let Γ' be the semidirect product $\Gamma_0 \rtimes \mathbb{Z}$ defined by the group law

$$(x, a) \cdot (y, b) = (x \gamma^a y \gamma^{-a}, a + b)$$

for $x, y \in \Gamma_0$ and $a, b \in \mathbb{Z}$. Define a map $\rho' : \Gamma' \rightarrow H$ by $\rho'((x, a)) = \rho_0(x) h^a$ for all $(x, a) \in \Gamma'$. The assumption guarantees that ρ' is a homomorphism of groups. It is clear that the kernel of the natural surjection $\pi : \Gamma' \rightarrow \Gamma_1 = \Gamma_0 \cdot \gamma^\mathbb{Z}$ is the cyclic subgroup generated by the element $(\gamma^n, -n)$ since on the normal subgroup $\Gamma_0 \subseteq \Gamma'$ this surjection is the identity and modulo Γ_0 it is the natural projection $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ (so its kernel cannot contain (γ_0, i) for $\gamma_0 \in \Gamma$ and $0 < i < n$, and for $i = 0$ necessarily $\gamma_0 = 1$). Since the restriction of ρ' to $\ker(\pi)$ is trivial, $\rho' = \rho_1 \circ \pi$ for a unique homomorphism $\rho_1 : \Gamma_1 \rightarrow H$. \square

Let F and K be number fields. Let $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ be an algebraic Hecke character, and let $\epsilon_{\text{alg}} : \underline{F}^\times \rightarrow \underline{K}^\times$ be the algebraic part of ϵ . Let E be a subfield of F such that ϵ_{alg} factors through the norm map $\text{Nm}_{F/E} : \underline{F}^\times \rightarrow \underline{E}^\times$; i.e., there exists a \mathbb{Q} -rational homomorphism $\chi_{\text{alg}} : \underline{E}^\times \rightarrow \underline{K}^\times$ such that $\epsilon_{\text{alg}} = \chi_{\text{alg}} \circ \text{Nm}_{F/E}$. (Beware that this is weaker than saying $\epsilon = \chi \circ \text{Nm}_{F/E}$ for an algebraic Hecke character $\chi : \mathbb{A}_E^\times \rightarrow K^\times$ with algebraic part χ_{alg} since an algebraic Hecke character is only determined by its algebraic part up to a finite order character. Moreover, χ_{alg} may not even be the algebraic part of an algebraic Hecke character.)

(4.11) Theorem *Using notation and hypotheses as above, let v be a finite place of F such that ϵ is unramified at v and let w be the place of E induced by v . Suppose that an element $\beta \in K^\times$ satisfies $\beta^{[\kappa_v : \kappa_w]} = \epsilon(\pi_v)$, where π_v is a local uniformizer of $\mathcal{O}_{F,v}$. There exists a finite extension \tilde{E} of E , a place \tilde{w} of \tilde{E} above w , and an algebraic Hecke character $\delta : \mathbb{A}_{\tilde{E}}^\times \rightarrow K^\times$ with the following properties.*

- (i) $[\kappa_{\tilde{w}} : \kappa_w] = 1$; i.e., the degree of the residue field extension for \tilde{w} over w is 1.
- (ii) The algebraic part of δ is equal to $\chi_{\text{alg}} \circ \text{Nm}_{\tilde{E}/E}$.
- (iii) The algebraic Hecke character δ is unramified at \tilde{w} , and $\delta(\pi_{\tilde{w}}) = \beta$, where $\pi_{\tilde{w}}$ is a uniformizer of $\mathcal{O}_{\tilde{E},\tilde{w}}$.

PROOF. Let F'/F be a finite extension that is Galois over E , and choose a place v' on F' over v . The composition ϵ' of ϵ with $\text{Nm}_{F'/F}$ on ideles is an algebraic Hecke character that is unramified at v' and has algebraic part $\epsilon_{\text{alg}} \circ \text{Nm}_{F'/F} = \chi_{\text{alg}} \circ \text{Nm}_{F'/E}$. If $\pi_{v'} \in \mathcal{O}_{F',v'}$ is a uniformizer then $\text{Nm}_{F'/F}(\pi_{v'})$ is an $\mathcal{O}_{F,v}^\times$ -multiple of $\pi_v^{[\kappa_{v'} : \kappa_v]}$, so $\epsilon'(\pi_{v'}) = \beta^{[\kappa_{v'} : \kappa_w]}$. Thus, by replacing F , ϵ , and v with F' , ϵ' , and v' we may and do assume that F is Galois over E . Choose an arithmetic Frobenius element σ in a decomposition $D_{\tilde{v}|w} \subseteq \text{Gal}(F^{\text{ab}}/E)$; i.e., σ induces $x \mapsto x^{q_w}$ on the residue field of an extension \tilde{v} of v to F^{ab} , with $q_w = \#\kappa_w$. Let ℓ be a prime number which is prime to v , and let $\psi_\ell : \text{Gal}(F^{\text{ab}}/F) \rightarrow K_\ell^\times$ be the ℓ -adic character attached to the algebraic Hecke character ϵ as in Lemma 4.8. As we saw in Lemma 4.8, ψ_ℓ is locally algebraic above ℓ with $\epsilon_{\text{alg}}^{-1}$ as its algebraic part above ℓ . Choose $M \geq 1$ such that $\sigma^{f(v|w)M}$ lies in the decomposition group $D_{\tilde{v}|v} \subseteq \text{Gal}(F^{\text{ab}}/F)$ at \tilde{v} , with $f(v|w) := [\kappa_v : \kappa_w]$. This agrees modulo the inertia group $I_{\tilde{v}|v}$ with the M th power of an arithmetic Frobenius element in $D_{\tilde{v}|v}$, so by unramifiedness of ψ_ℓ at v we compute $\psi_\ell(\sigma^{f(v|w)M}) = \psi_\ell(\text{Frob}_v^M) = \epsilon(\pi_v)^M = \beta^{f(v|w)M}$.

Since F/E is Galois, $\sigma \in \text{Gal}(F^{\text{ab}}/E)$ acts on $\text{Gal}(F^{\text{ab}}/F)$ by conjugation. Consider the conjugate of ψ_ℓ by σ ; i.e., the continuous homomorphism ${}^\sigma\psi_\ell : \text{Gal}(F^{\text{ab}}/F) \rightarrow K_\ell^\times$ defined by $\tau \mapsto \psi_\ell(\sigma^{-1}\tau\sigma)$. Clearly ${}^\sigma\psi_\ell$ is unramified at all but finitely many places and is locally algebraic above ℓ , with algebraic part above ℓ given by composing the algebraic part of ψ_ℓ above ℓ with the action by $\sigma|_F$ on F_ℓ^\times . Because ϵ_{alg} factors through $\text{Nm}_{F/E}$, it is invariant under the action of $\sigma|_F \in \text{Gal}(F/E)$. Hence, the algebraic part of ${}^\sigma\psi_\ell$ above ℓ is also equal to $\epsilon_{\text{alg}}^{-1}$. Therefore, by Remark 4.6(ii), there exists a finite abelian extension field F_1 of F which is Galois over E such that ${}^\sigma\psi_\ell$ coincides with ψ_ℓ on $\text{Gal}(F^{\text{ab}}/F_1)$. Replacing F_1 by a finite extension that is abelian over F and Galois over E with sufficiently divisible degree over F_1 (e.g., a sufficiently large ray class field of F), we may assume (by the relationship between finite-index subgroups of \mathbb{Z} and open subgroups of $\widehat{\mathbb{Z}}$) that there exists a positive integer N_1 such that $\sigma^{\mathbb{Z}} \cap \text{Gal}(F^{\text{ab}}/F_1) = \sigma^{f(v|w)MN_1\mathbb{Z}}$.

Let $\tilde{E} \subseteq F_1$ be the subfield over E that is the fixed field of the cyclic group $\langle \sigma|_{F_1} \rangle \subseteq \text{Gal}(F_1/E)$ with order $f(v|w)MN_1$. Since $\psi_\ell(\sigma^{f(v|w)MN_1}) = \beta^{f(v|w)MN_1}$, by applying Lemma

4.10 with $\Gamma_0 = \text{Gal}(F^{\text{ab}}/F_1)$, $\Gamma = \text{Gal}(F^{\text{ab}}/E)$, $\gamma = \sigma$, and $n = f(v|w)MN_1$, we see that there is a unique continuous homomorphism $\tilde{\psi}_\ell : \text{Gal}(F^{\text{ab}}/\tilde{E}) \rightarrow K_\ell^\times$ which coincides with ψ_ℓ on $\text{Gal}(F^{\text{ab}}/F_1)$ and such that $\tilde{\psi}_\ell(\sigma) = \beta$. In particular, $\tilde{\psi}_\ell$ is unramified at all but finitely many places of \tilde{E} since ψ_ℓ is unramified at all but finitely many places of F and the finite extension F_1/\tilde{E} is unramified at all but finitely many places. Let \tilde{w} be the restriction to \tilde{E} of the place \tilde{v} on F^{ab} , so $\sigma \in D_{\tilde{v}|\tilde{w}}$. Since $\text{Gal}(F_1/\tilde{E}) \subseteq \text{Gal}(F_1/E)$ is the subgroup generated by $\sigma|_{F_1}$, we have that $\kappa_w \subseteq \kappa_{\tilde{w}}$ but $\kappa_{\tilde{w}}$ has trivial action by the automorphism $x \mapsto x^{q_w}$ induced by $\sigma|_{F_1}$. Hence, $\kappa_w = \kappa_{\tilde{w}}$, so (i) holds. Thus, $q_{\tilde{w}} = q_w$, so the element $\sigma \in D_{\tilde{v}|\tilde{w}} \subseteq \text{Gal}(F^{\text{ab}}/\tilde{E})$ is an arithmetic Frobenius element in this decomposition group. Beware that even though $\sigma|_{F_1}$ generates $\text{Gal}(F_1/\tilde{E})$, we do not see how to avoid the possibility that F_1/\tilde{E} is ramified at the restriction v_1 of \tilde{v} to F_1 (especially if F/E is ramified at v). Thus, we will have to do some work to check that the algebraic Hecke character δ that we shall construct is unramified at \tilde{w} .

By construction, the continuous K_ℓ^\times -valued character $\tilde{\psi}'_\ell$ of $\text{Gal}(\tilde{E}^{\text{ab}}/\tilde{E})$ induced by the continuous homomorphism $\tilde{\psi}_\ell : \text{Gal}(F^{\text{ab}}/\tilde{E}) \rightarrow K_\ell^\times$ is locally algebraic above ℓ , with algebraic part $\chi_{\text{alg}}^{-1} \circ \text{Nm}_{\tilde{E}/E}$ because we can compute the algebraic part by working near the identity (such as on the open image of $\text{Gal}(F^{\text{ab}}/F_1)$) and the relative norm map goes over to “restriction” on Galois groups via class field theory. Since the continuous $\tilde{\psi}'_\ell$ is unramified at all but finitely many places, the proof of Lemma 4.9 (especially the analysis of open kernels) therefore gives that the continuous homomorphism $\delta : \mathbb{A}_{\tilde{E}}^\times \rightarrow K_\ell^\times$ defined by the formula

$$\delta(x) = \tilde{\psi}'_\ell(r_{\tilde{E}}(x)) \cdot \chi_{\text{alg}}(\text{Nm}_{\tilde{E}/E}(x_\ell))$$

for $x \in \mathbb{A}_{\tilde{E}}^\times$ with ℓ -adic component $x_\ell \in \tilde{E}_\ell^\times$ is an algebraic Hecke character of \tilde{E} with values in the finite product of fields K_ℓ^\times , and that δ has algebraic part $\chi_{\text{alg}} \circ \text{Nm}_{\tilde{E}/E}$. In particular, δ has open kernel and hence is continuous with respect to the discrete topology on K_ℓ^\times .

Let U be the open subgroup $\tilde{E}^\times \cdot \text{Nm}_{F_1/\tilde{E}}(\mathbb{A}_{F_1}^\times)$ of finite index in $\mathbb{A}_{\tilde{E}}^\times$, and let $\pi_{\tilde{w}}$ be a uniformizer of $\mathcal{O}_{\tilde{E}, \tilde{w}}$ chosen such that the arithmetic Frobenius element $r_{\tilde{E}}(\pi_{\tilde{w}}) \in \text{Gal}(\tilde{E}^{\text{ab}}/\tilde{E})$ at \tilde{w} is equal to the arithmetic Frobenius element $\sigma|_{\tilde{E}^{\text{ab}}}$. Such a $\pi_{\tilde{w}}$ can be found because the profinite unit group $\mathcal{O}_{\tilde{w}}^\times$ surjects onto the inertia subgroup of $\text{Gal}(\tilde{E}_{\tilde{w}}^{\text{ab}}/\tilde{E}_{\tilde{w}})$. The idele group $\mathbb{A}_{\tilde{E}}^\times$ is generated by U and $\pi_{\tilde{w}}$ because $\text{Gal}(F_1/\tilde{E})$ is generated by $\sigma|_{F_1}$. Thus, to show that δ takes its values in $K^\times \subseteq K_\ell^\times$ it suffices to compute that $\delta(\pi_{\tilde{w}}) \in K^\times$ and that $\delta|_U$ is valued in K^\times . Since $\ell \nmid \tilde{w}$ (as $\ell \nmid v$), by the definitions of δ , $\tilde{\psi}_\ell$, and $\pi_{\tilde{w}}$ we have

$$\delta(\pi_{\tilde{w}}) = \tilde{\psi}'_\ell(r_{\tilde{E}}(\pi_{\tilde{w}})) = \tilde{\psi}'_\ell(\sigma|_{\tilde{E}^{\text{ab}}}) = \tilde{\psi}_\ell(\sigma) = \beta \in K^\times.$$

Meanwhile, for any element $x \in U$, written in the form $x = \text{Nm}_{F_1/\tilde{E}}(y) \cdot z$ with $y \in \mathbb{A}_{F_1}^\times$ and $z \in \tilde{E}^\times$, since $r_{\tilde{E}}(\tilde{E}^\times) = \{1\}$ we have

$$\begin{aligned} \delta(x) &= \tilde{\psi}'_\ell(r_{\tilde{E}}(x)) \cdot \chi_{\text{alg}}(\text{Nm}_{\tilde{E}/E}(x_\ell)) \\ &= \psi_\ell(r_F(\text{Nm}_{F_1/F}(y))) \cdot \chi_{\text{alg}}(\text{Nm}_{F/E}(\text{Nm}_{F_1/F}(y_\ell))) \cdot \chi_{\text{alg}}(\text{Nm}_{\tilde{E}/E}(z_\ell)) \\ &= \epsilon(\text{Nm}_{F_1/F}(y)) \cdot \chi_{\text{alg}}(\text{Nm}_{\tilde{E}/E}(z)) \in K^\times, \end{aligned}$$

where the final equality uses the construction of ϵ from ψ_ℓ as in the proof of Lemma 4.9 (since $\epsilon_{\text{alg}} = \chi_{\text{alg}} \circ \text{Nm}_{F/E}$). Thus, indeed $\delta(\mathbb{A}_{\tilde{E}}^\times) \subseteq K^\times$.

We have shown that δ is an algebraic Hecke character satisfying the required properties (i)–(iii), except for verifying that δ is unramified at \tilde{w} . The key to settling this remaining

issue even if F_1/\tilde{E} is ramified at \tilde{w} is to exploit the cyclicity of F_1/\tilde{E} , and more specifically the Hasse Norm Theorem for cyclic extensions of number fields. For a local unit $u \in \mathcal{O}_{\tilde{E},\tilde{w}}^\times$, we have to prove $\delta(u) = 1$ when u is viewed in $\mathbb{A}_{\tilde{E}}^\times$ in the natural manner. We can write $u = z \cdot \text{Nm}_{F_1/\tilde{E}}(y) \cdot \pi_{\tilde{w}}^i$ for some $i \in \mathbb{Z}$, $z \in \tilde{E}^\times$, and $y \in \mathbb{A}_{F_1}^\times$. In particular, since the \tilde{E} -idele $u\pi_{\tilde{w}}^{-i}$ has trivial local component at every place away from \tilde{w} , it follows that $z \in \tilde{E}^\times$ is a local norm from F_1 at every place away from \tilde{w} . By the triviality of $r_{\tilde{E}}$ on \tilde{E}^\times , z is a local norm at \tilde{w} . Hence, by the Hasse Norm Theorem for cyclic extensions, z is a global norm: $z = \text{Nm}_{F_1/E}(z_1)$ for some $z_1 \in F_1^\times$. Thus, by replacing y with $z_1 y$ we can assume $z = 1$. There is a unique place v_1 of F_1 over \tilde{w} because $\sigma \in D_{\tilde{w}|\tilde{w}} \subseteq \text{Gal}(F^{\text{ab}}/\tilde{E})$ and $\text{Gal}(F_1/\tilde{E})$ is generated by $\sigma|_{F_1}$. We therefore have $u = \text{Nm}_{F_1,v_1/\tilde{E}_{\tilde{w}}}(y_1)\pi_{\tilde{w}}^i$, where y_1 is the v_1 -component of the F_1 -idele y .

Let $\pi_{v_1} \in \mathcal{O}_{F_1,v_1}^\times$ be a uniformizer, so there is a unique $j \in \mathbb{Z}$ and $u_1 \in \mathcal{O}_{F_1,v_1}^\times$ such that $y_1 = \pi_{v_1}^j u_1$. Since $\text{Nm}_{F_1,v_1/\tilde{E}_{\tilde{w}}}(\pi_{v_1})$ is an $\mathcal{O}_{\tilde{E},\tilde{w}}^\times$ -multiple of $\pi_{\tilde{w}}^{f(v_1|\tilde{w})}$, the condition $\text{ord}_{\tilde{w}}(u) = 0$ forces $i = -f(v_1|\tilde{w})j = -f(v_1|w)j = -f(v_1|v)f(v|w)j$. Hence,

$$\delta(u) = \delta(\text{Nm}_{F_1/\tilde{E}}(y_1))\delta(\pi_{\tilde{w}})^i = \epsilon(\text{Nm}_{F_1/F}(y_1))\beta^{-f(v_1|v)f(v|w)j} = \epsilon(\text{Nm}_{F_1/F}(y_1))\epsilon(\pi_v)^{-f(v_1|v)j}$$

where y_1 is viewed as an F_1 -idele supported at v_1 (so $\text{Nm}_{F_1/F}(y_1) = \text{Nm}_{F_1,v_1/F_v}(y_1)$ as an F -idele supported at v). Since ϵ is unramified at v , $\epsilon(\text{Nm}_{F_1,v_1/F_v}(y_1)) = \epsilon(\text{Nm}_{F_1,v_1/F_v}(\pi_{v_1}))^j$. Thus, we just have to show $\epsilon(\pi_v)^{f(v_1|v)} = \epsilon(\text{Nm}_{F_1,v_1/F_v}(\pi_{v_1}))$, and this follows from the unramifiedness of ϵ at v and the fact that the (normalized) v -adic ordinal of $\text{Nm}_{F_1,v_1/F_v}(\pi_{v_1})$ is $f(v_1|v)$. \square

(4.12) Remark In the final part of the proof of Theorem 4.11, to prove the unramifiedness of δ at \tilde{w} , we had to do some extra work with the Hasse Norm Theorem to overcome the possibility that F_1/\tilde{E} could be ramified at its unique place above \tilde{w} . Let us indicate an alternative procedure to bypass this difficulty by using the Grunwald–Wang theorem [1, Ch. X, Thm. 5]. Let v_1 be the unique place of F_1 above \tilde{w} , and let $e(v_1|\tilde{w})$ be the ramification index. By the Grunwald–Wang theorem, there exists a cyclic extension F_2/F_1 which is unramified at v_1 such that the residual degree $f(v_1, F_2/F_1)$ is a multiple of $e(v_1|\tilde{w})$. Let F_3/F_2 be a Galois closure of F_2 over \tilde{E} , so F_3/F_1 is abelian and unramified over v_1 . Let v_2 be a place of F_2 above v_1 , and let v_3 be a place of F_3 above v_2 . Consider the short exact sequence $1 \rightarrow I_{v_1|\tilde{w}} \rightarrow D_{v_1|\tilde{w}} \rightarrow \text{Gal}(\kappa_{v_1}/\kappa_{\tilde{w}}) \rightarrow 1$ for the decomposition group $D_{v_1|\tilde{w}}$. The short exact sequence $1 \rightarrow I_{v_3|\tilde{w}} \rightarrow D_{v_3|\tilde{w}} \rightarrow \text{Gal}(\kappa_{v_3}/\kappa_{\tilde{w}}) \rightarrow 1$ for the decomposition group $D_{v_3|\tilde{w}}$ is the pullback of the previous short exact sequence by the natural surjection $\text{Gal}(\kappa_{v_3}/\kappa_{\tilde{w}}) \twoheadrightarrow \text{Gal}(\kappa_{v_1}/\kappa_{\tilde{w}})$ because $e(v_3|\tilde{w}) = e(v_1|\tilde{w})$. This pullback sequence splits (as a semi-direct product) because $\text{Gal}(\kappa_{v_3}/\kappa_{\tilde{w}})$ is a cyclic group whose cardinality is a multiple of the cardinality of $D_{v_1|\tilde{w}}$; here we use that F_2/F_1 was chosen so that $e(v_1|\tilde{w}) \mid [\kappa_{v_2} : \kappa_{v_1}]$. Thus, there exists $\sigma_3 \in D_{v_3|\tilde{w}}$ that maps to the arithmetic Frobenius element in $\text{Gal}(\kappa_{v_3}/\kappa_{\tilde{w}})$ and for which the subgroup generated by σ_3 is a lifting of $\text{Gal}(\kappa_{v_3}/\kappa_{\tilde{w}})$ in $D_{v_3|\tilde{w}}$. Let E_3 be the subfield of F_3 fixed by σ_3 , so v_3 is the only place on F_3 over its restriction w_3 in E_3 . The extension F_3/E_3 is unramified over w_3 , by consideration of field degrees (residually and generically). The statement of Theorem 4.11 holds with (\tilde{E}, \tilde{w}) replaced by (E_3, w_3) ; that δ is unramified at w_3 is easy to see because F_3/E_3 is unramified.

§5. Theory of complex multiplication

We now review part of the theory of complex multiplication due to Shimura and Taniyama, and then we use it to translate Theorem 4.11 into a statement concerning CM-liftings of abelian varieties up to isogeny. The references for this section are [26], [25], [24], [16], [19], and [6].

(5.1) Theorem *Let $F \subseteq \overline{\mathbb{Q}}$ be a number field. Let A be an abelian variety over F . Let K be a CM field such that $[K : \mathbb{Q}] = 2 \cdot \dim(A)$. Let $\alpha : K \rightarrow \text{End}^0(A)$ be a ring homomorphism; i.e., A has CM by K over F . Let Φ be the CM-type of A . The following properties hold.*

- (i) *The reflex field $E \subseteq \overline{\mathbb{Q}}$ of the CM-type Φ is contained in F .*
- (ii) *There exists a unique algebraic Hecke character $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ such that for every prime number ℓ , the continuous homomorphism $\psi_\ell : \text{Gal}(F^{\text{ab}}/F) \rightarrow K_\ell^\times$ attached to ϵ is equal to the ℓ -adic representation of $\text{Gal}(F^{\text{ab}}/F)$ attached to the ℓ -power torsion points of A .*
- (iii) *The algebraic part of the algebraic Hecke character ϵ is the map $N_\Phi \circ \text{Nm}_{F/E}$, where $N_\Phi : \text{Res}_{E/\mathbb{Q}}(\mathbb{G}_m) \rightarrow \text{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$ is the reflex norm.*
- (iv) *Let v be a finite place of F . The abelian variety A has good reduction at v if and only if the algebraic Hecke character ϵ is unramified at v .*
- (v) *If v is a finite place of F where A has good reduction, say with reduction \overline{A} over κ_v , then $\epsilon(\pi_v) = \text{Fr}_{\overline{A}, q_v}$, where π_v is a uniformizer of \mathcal{O}_{F_v} and $q_v = \#\kappa_v$.*

Note that Theorem 5.1 is insensitive to K -linear isogenies in A over F , so there is no loss of generality in assuming that the CM order is \mathcal{O}_K . Part (i) is immediate from the definition of the reflex field, and (ii) and (iii) amount to a reformulation of the Main Theorem of complex multiplication as stated in [26]. Part (iv) is proved in §7 of [25] as a consequence of this main theorem. Finally, (v) follows from (ii) and (iv). See also [24], (II-25)–(II-28); [16], Chapter 4, §1; and [6], §3.

(5.2) Theorem *Let K be a CM field with $[K : \mathbb{Q}] = 2g$. Let Φ be a CM-type for K valued in a fixed algebraic closure $\overline{\mathbb{Q}}$ and let $E \subseteq \overline{\mathbb{Q}}$ be the reflex field of (K, Φ) . Let F/E be a finite extension. Let $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ be an algebraic Hecke character whose algebraic part is the composite map $N_\Phi \circ \text{Nm}_{F/E}$, where N_Φ is the reflex norm associated to (K, Φ) .*

There exists a g -dimensional abelian variety A over F and a ring homomorphism $\alpha : K \rightarrow \text{End}^0(A)$ such that Φ is the CM-type of (A, α) and ϵ is the algebraic Hecke character attached to (A, α) as in Theorem 5.1(ii). Moreover (A, α) is unique up to K -linear F -isogeny.

(5.3) Remark This theorem is a converse of Theorem 5.1 and a known fact. For instance, it is a consequence of the motivic theory of complex multiplication. More specifically, it is a consequence of [8], Prop. E.1, pp. 273–275. Also, it is proved in Chapter 5, §5 of [16] using an older style of algebraic geometry and the traditional analytic formulation of the Main Theorem of complex multiplication (as stated in Theorem 6.1 of Chapter 3 of loc. cit.). For the reader who prefers a purely algebraic proof of this algebraic result, using modern algebro-geometric terminology, we have provided such an argument in the appendix.

We are now in position to prove Theorem 1.6. Let us first recall the statement.

(5.4) Proposition *Let K be a CM field with degree $2g$ over \mathbb{Q} . Let $q = p^r$, where p is a prime number. Let B be an isotypic abelian variety of dimension g over a finite field \mathbb{F}_q with size q , and let $\alpha_B : K \rightarrow \text{End}^0(B)$ be a ring homomorphism. Suppose that there exists a p -adic CM-type $\Phi \subseteq \text{Hom}_{\text{ring}}(K, \overline{\mathbb{Q}}_p)$ of K such that the residual reflex condition in §1.5 is satisfied for (K, Φ) . Let $E \subseteq \overline{\mathbb{Q}}_p$ be the reflex field of (K, Φ) , and let w be the induced p -adic place on E .*

There exists a finite extension \tilde{E}/E inside of $\overline{\mathbb{Q}}_p$, an abelian variety A over \tilde{E} , and a ring homomorphism $\alpha : K \rightarrow \text{End}^0(A)$ such that the following statements hold.

- (i) *The residue field $\kappa_{\tilde{w}}$ of \tilde{E} at the place \tilde{w} induced from $\overline{\mathbb{Q}}_p$ is isomorphic to \mathbb{F}_q .*
- (ii) *The p -adic CM-type of (A, α) is Φ .*
- (iii) *The abelian variety A over \tilde{E} has good reduction at \tilde{w} .*
- (iv) *Via a suitable isomorphism $\mathbb{F}_q \simeq \kappa_{\tilde{w}}$, B is K -linearly isogenous to the reduction of A at \tilde{w} .*

Note that in (iv) the choice of isomorphism $\mathbb{F}_q \simeq \kappa_{\tilde{w}}$ does not matter, since B and $B^{(p)}$ are K -linearly isogenous over \mathbb{F}_q via the relative Frobenius map for B .

PROOF. This proposition is a consequence of Theorems 4.11, 5.1, and 5.2, as we explain in the argument below.

The classical theory of complex multiplication in [26] provides an abelian variety X_1 of dimension g over a finite extension L_1 of \mathbb{Q}_p within $\overline{\mathbb{Q}}_p$ and a homomorphism $\xi_1 : \mathcal{O}_K \rightarrow \text{End}(X_1)$ such that (X_1, ξ_1) has CM-type Φ . In particular, the reflex field $E \subseteq \overline{\mathbb{Q}}_p$ is a subfield of L_1 such that the canonical p -adic absolute value on L_1 induces the p -adic place w on E . By replacing L_1 with a finite extension if necessary, we can assume that X_1 has good reduction over \mathcal{O}_L and that the size q_1 of the residue field κ_1 of L_1 is a power of q . Let $\pi_1 \in \mathcal{O}_K$ be the element whose action on the reduction \overline{X}_1 over κ_1 is the q_1 -Frobenius endomorphism (so it is a q_1 -Weil number). The Shimura–Taniyama formula gives

$$\frac{\text{ord}_v(\pi_1)}{\text{ord}_v(q_1)} = \frac{\#\{\phi \in \Phi \mid \phi \text{ induces } v \text{ on } K\}}{[K_v : \mathbb{Q}_p]}$$

for all p -adic places v of K . But the first part of the residual reflex condition is the hypothesis on the p -adic CM-type Φ that the right side of this identity is equal to $\text{ord}_v(\text{Fr}_{B,q})/\text{ord}_v(q)$ for each v (where $\text{Fr}_{B,q}$ is identified with a nonzero element of \mathcal{O}_K via the CM-structure on B over \mathbb{F}_q). Since q_1 is a power of q , we can choose an embedding $\mathbb{F}_q \hookrightarrow \kappa$ to make sense of $\text{Fr}_{B_\kappa, q_1}$, and as an element of K this q_1 -Frobenius endomorphism is $\text{Fr}_{B,q}^{[\mathbb{F}_{q_1} : \mathbb{F}_q]}$. Hence,

$$\frac{\text{ord}_v(\pi_1)}{\text{ord}_v(q_1)} = \frac{\text{ord}_v(\text{Fr}_{B,q})}{\text{ord}_v(q)} = \frac{\text{ord}_v(\text{Fr}_{B_\kappa, q_1})}{\text{ord}_v(q_1)},$$

so the q_1 -Weil numbers $\pi_1, \text{Fr}_{B_\kappa, q_1} \in \mathcal{O}_K$ have the same order at each p -adic place of \mathcal{O}_K . Their ratio is therefore a root of unity, so by replacing L_1 with a suitable unramified extension (so as to replace q_1 with a suitable power) we can arrange that $\pi_1 = \text{Fr}_{B_\kappa, q_1}$ inside of \mathcal{O}_K .

By Honda–Tate theory, the g -dimensional isotypic abelian varieties \overline{X}_1 and B_κ over κ are therefore isogenous. Although a choice of κ -isogeny $\overline{X}_1 \rightarrow B_\kappa$ may not be K -linear, it at least carries $\pi_1 = \text{Fr}_{\overline{X}_1, q_1}$ to $\text{Fr}_{B_\kappa, q_1}$. In other words, the induced isomorphism

$$\theta : \text{End}^0(\overline{X}_1) \simeq \text{End}^0(B_\kappa)$$

of simple \mathbb{Q} -algebras may not be K -linear but it is linear over the subfield $Z \subseteq K$ generated by the q_1 -Frobenius endomorphisms in each algebra. But Z is the center of these simple \mathbb{Q} -algebras in which K is a maximal commutative subfield, so the Z -linearity allows us to use the Skolem–Noether theorem to find a unit $u \in \text{End}^0(B_\kappa)^\times$ such that composing θ with conjugation by u is a K -algebra map. In other words, if we compose the initial κ -isogeny with a suitable self-isogeny of B_κ (corresponding to a nonzero \mathbb{Z} -multiple of u) we can arrange that the κ -isogeny $\overline{X}_1 \rightarrow B_\kappa$ is K -linear. Finally, by replacing L_1 with a further finite extension if necessary we can ensure that the pair (X_1, ξ_1) descends to a number field $F \subseteq L_1$, and by increasing F we can ensure that L_1 is identified with the completion F_v at the induced p -adic place v on F . In particular, $E \subseteq F$ and v on F restricts to w on E .

To summarize, by using the first part of the residual reflex condition we have constructed a finite extension F/E inside of $\overline{\mathbb{Q}}_p$ and a CM abelian variety (A_1, α_1) over F with good reduction at the induced p -adic place v of F such that the associated p -adic CM-type is (K, Φ) and the reduction \overline{A}_1 at v is K -linearly isogenous to B_{κ_v} via a choice of embedding $\mathbb{F}_q \hookrightarrow \kappa_v$. Such an isogeny carries $\text{Fr}_{\overline{A}_1, q_v}$ to $\text{Fr}_{B_{\kappa_v}, q_v}$ as endomorphisms, and so the corresponding elements of \mathcal{O}_K (via the CM-structures) are equal, due to K -linearity of the isogeny.

Pick a finite extension E_1 of E that is linearly disjoint from F over E and which has a place w_1 above w such that κ_{w_1} is isomorphic to \mathbb{F}_q . Choose an E -embedding $E_1 \rightarrow \overline{\mathbb{Q}}_p$ inducing w_1 . By replacing F with the composite field $E_1 \otimes_E F \subseteq \overline{\mathbb{Q}}_p$, we may assume that F contains a subfield E'/E on which the induced place w' from v satisfies $\kappa_{w'} \simeq \mathbb{F}_q$. By Theorem 5.1, we get an algebraic Hecke character $\epsilon : \mathbb{A}_F^\times \rightarrow K^\times$ attached to (A_1, α_1) which has $N_\Phi \circ \text{Nm}_{F/E}$ as its algebraic part and is unramified at v with $\epsilon(\pi_v) = \text{Fr}_{(B, \alpha_B)_{\kappa_v}}$.

Apply Theorem 4.11 to (ϵ, E', β) with $\chi_{\text{alg}} = N_\Phi \circ \text{Nm}_{E'/E}$ and β equal to the element of \mathcal{O}_K corresponding to $\text{Fr}_{B, q}$ via α_B (so $\beta^{[\kappa_v : \kappa_{w'}]} = \beta^{[\kappa_v : \mathbb{F}_q]} = \text{Fr}_{(B, \alpha_B)_{\kappa_v}} = \epsilon(\pi_v)$). This provides a finite extension \tilde{E}/E' , a place \tilde{w} above w' , and an algebraic Hecke character $\delta : \mathbb{A}_{\tilde{E}}^\times \rightarrow K^\times$ with the properties stated in Theorem 4.11. Hence, $\delta_{\text{alg}} = \chi_{\text{alg}} \circ \text{Nm}_{\tilde{E}/E_1} = N_\Phi \circ \text{Nm}_{\tilde{E}/E}$, δ is unramified at \tilde{w} , $\delta(\pi_{\tilde{w}}) = \beta = \text{Fr}_{B, q}$, and (\tilde{E}, \tilde{w}) has property (i). Fix an E' -embedding of \tilde{E} into $\overline{\mathbb{Q}}_p$ inducing \tilde{w} on \tilde{E} . By Theorem 5.2 (and Theorem 5.1(iv),(v)), the algebraic Hecke character δ comes from a pair (A, α) over \tilde{E} with the required properties (ii)–(iv). Let us briefly explain how to get (iv). Let \overline{A} denote the reduction of A at \tilde{w} and let $\pi \in \mathcal{O}_K$ denote $\delta(\pi_{\tilde{w}})$, so the respective CM-structures $\overline{\alpha}$ and α_B on \overline{A} and B satisfy $\overline{\alpha}(\pi) = \text{Fr}_{\overline{A}, q}$ and $\alpha_B(\pi) = \text{Fr}_{B, q}$. Since \overline{A} is $\kappa_{\tilde{w}}$ -isotypic and B is \mathbb{F}_q -isotypic (due to the existence of CM-structures), it follows from Honda–Tate theory that there is an isogeny between \overline{A} and B over any isomorphism $\kappa_{\tilde{w}} \simeq \mathbb{F}_q$. We want to find such an isogeny that is K -linear. At least any isogeny respects the q -Frobenius endomorphisms, and so (via the CM-structures $\overline{\alpha}$ and α_B) is linear over the subfield $\mathbb{Q}(\pi) \subseteq K$. But via $\overline{\alpha}$ and α_B the subfield $\mathbb{Q}(\pi)$ is the center of each of the endomorphism algebras of \overline{A} and B , so we can use the Skolem–Noether theorem as we did earlier in this proof to modify the isogeny by a suitable self-isogeny of B to get a K -linear isogeny. \square

§6. Local methods

It is possible to prove Proposition 5.4 by replacing the global Theorem 5.2 with purely local methods (but still using the classical theory of complex multiplication to construct an abelian variety with good reduction over a local field admitting a specified CM type and Frobenius endomorphism on the reduction). After using local methods to prove a local version of Propo-

sition 5.4 (in which the number field \tilde{E} is replaced with a p -adic field) we will formally deduce the global version of the proposition (over number fields) from the local version. First we establish a local analogue of Theorem 4.11, using the argument in Remark 4.12.

(6.1) Lemma *Let E_w be a finite extension field of \mathbb{Q}_p , and let F_v be a finite extension field of E_w . Let K be a number field, and let ϕ be an element of K^\times . Let $\epsilon_v : F_v^\times \rightarrow K^\times$ be an unramified character. Assume that $\epsilon_v(\pi_v^n) = \phi^{n[\kappa_v:\kappa_w]}$ for some fixed $n \geq 1$, with π_v a uniformizer of F_v . There exists a finite extension \tilde{F}_v/F_v and an intermediate extension $\tilde{E}_w \subseteq \tilde{F}_v$ over E_w such that the following conditions hold.*

- (i) *The extension \tilde{F}_v/\tilde{E}_w is unramified.*
- (ii) *The residue field extension $\kappa_{\tilde{w}}/\kappa_w$ is trivial; i.e., \tilde{E}_w/E_w is totally ramified.*
- (iii) $\epsilon_v(\text{Nm}_{\tilde{F}_v/F_v}(\pi_{\tilde{v}})) = \phi^{[\kappa_{\tilde{v}}:\kappa_w]}$
- (iv) *Choose a uniformizer $\pi_{\tilde{w}}$ of \tilde{E}_w . There is a unique character $\epsilon_{\tilde{w}} : \tilde{E}_w^\times \rightarrow K^\times$ such that $\epsilon_v \circ \text{Nm}_{\tilde{F}_v/F_v} = \epsilon_{\tilde{w}} \circ \text{Nm}_{\tilde{F}_v/\tilde{E}_w}$ and $\epsilon_{\tilde{w}}(\pi_{\tilde{w}}) = \phi$. Moreover, it is unramified.*

PROOF. Let F_1 be the unramified extension field of F_v of degree n , and let F_2 be the Galois closure of F_1 over E_w . Consider the short exact sequence of finite groups

$$1 \rightarrow I_{F_2/E_w} \rightarrow \text{Gal}(F_2/E_w) \rightarrow \text{Gal}(\kappa_{F_2}/\kappa_w) \rightarrow 1$$

where I_{F_2/E_w} is the inertia subgroup in $\text{Gal}(F_2/E_w)$. This is not necessarily a split extension, but it would be split if we replace F_2 by the unramified extension field F_3 of F_2 of degree $e(F_2/E_w)$, or more generally by any finite unramified extension field F_3 such that $[F_3 : F_2]$ is a multiple of the ramification index $e(F_2/E_w)$, because the short exact sequence $1 \rightarrow I_{F_3/E_w} \rightarrow \text{Gal}(F_3/E_w) \rightarrow \text{Gal}(\kappa_{F_3}/\kappa_w) \rightarrow 1$ is the pullback of the exact sequence $1 \rightarrow I_{F_2/E_w} \rightarrow \text{Gal}(F_2/E_w) \rightarrow \text{Gal}(\kappa_{F_2}/\kappa_w) \rightarrow 1$ by the natural surjection $\text{Gal}(\kappa_{F_3}/\kappa_w) \rightarrow \text{Gal}(\kappa_{F_2}/\kappa_w)$.

Take $\tilde{F}_v = F_3$. Choose a splitting $j : \text{Gal}(\kappa_{\tilde{v}}/\kappa_w) \rightarrow \text{Gal}(\tilde{F}_v/E_w)$ of the short exact sequence

$$1 \rightarrow I_{\tilde{F}_v/E_w} \rightarrow \text{Gal}(\tilde{F}_v/E_w) \rightarrow \text{Gal}(\kappa_{\tilde{v}}/\kappa_w) \rightarrow 1,$$

and let \tilde{E}_w be the subfield of \tilde{F}_v fixed by $j(\text{Gal}(\kappa_{\tilde{v}}/\kappa_w))$. The statements (i)–(iv) are all easy to check (for (iv) we use that the local norm map is surjective on local unit groups in the unramified case, and for (iii) we use that $n|[\kappa_{\tilde{v}}:\kappa_w]$ by construction of F_1). \square

Our aim is to remove the global Theorem 5.2 from the proof of Proposition 5.4. The construction of a CM abelian variety (A_1, α_1) with p -adic CM type (K, Φ) over a finite extension F/E inside of $\overline{\mathbb{Q}}_p$ goes as in the first two paragraphs of the proof of Proposition 5.4. In particular, A has good reduction at the place v on F over w induced by the inclusion $F \subseteq \overline{\mathbb{Q}}_p$ and moreover the residual extension κ_v/κ_w has \mathbb{F}_q as an intermediate extension such that the reduction \overline{A}_1 over κ_v is K -linearly isogenous to $B \otimes_{\mathbb{F}_q} \kappa_v$. Let $E'_{w'}/E_w$ be the intermediate unramified extension of E_w corresponding to \mathbb{F}_q/κ_w , and let ϵ_v be the restriction to F_v^\times of the algebraic Hecke character ϵ attached to the CM abelian variety (A_1, α_1) over F with CM-order \mathcal{O}_K .

By Lemma 4.8, Lemma 4.9 (see (3)), and Theorem 5.1(iii), the character

$$\psi_{p,v} : \text{Gal}(F_v^{\text{ab}}/F_v) \rightarrow \mathcal{O}_{K,p}^\times$$

attached to the p -divisible group $(A_1)_{F_v}[p^\infty]$ equipped with its K_p -action via α_1 is related to the character ϵ_v via the formula

$$\epsilon_v(x) = \psi_{p,v}(r_F(x)) \cdot N_\Phi(\mathrm{Nm}_{F_v/E_w}(x))$$

for all $x \in F_v^\times$. Apply Theorem 5.1(iv) and Lemma 6.1 to $(E'_{w'}, F_v, \epsilon_v, \phi, n)$, where $\phi = \alpha_B(\mathrm{Fr}_{B,q}) \in K^\times$ and $n = 1$. We obtain a finite extension \tilde{F}_v/F_v inside of $\overline{\mathbb{Q}}_p$, an intermediate extension $\tilde{E}_{\tilde{w}}$ in \tilde{F}_v over $E'_{w'}$, and a K^\times -valued unramified character $\epsilon_{\tilde{w}}$ of $\tilde{E}_{\tilde{w}}^\times$ satisfying the properties (i)–(iv) in Lemma 6.1. In particular, $\tilde{F}_v/\tilde{E}_{\tilde{w}}$ is unramified, $\kappa_{\tilde{w}} = \kappa_{w'} = \mathbb{F}_q$, and $\epsilon_{\tilde{w}}(\pi_{\tilde{w}}) = \alpha_B(\mathrm{Fr}_{B,q}) \in K^\times$.

Denote by \mathcal{A}_1 the abelian scheme over $\mathcal{O}_{\tilde{F}_v}$ extending the base change $(A_1)_{F_v}$, and endow it with the unique K -action (in the isogeny category) extending that defined on its generic fiber via α_1 . The p -divisible group $\mathcal{G}_1 = \mathcal{A}_1[p^\infty]$ over $\mathcal{O}_{\tilde{F}_v}$ is thereby endowed with a natural action by K_p in the isogeny category, and its generic fiber is given by the restriction to $\mathrm{Gal}(\tilde{F}_v^{\mathrm{ab}}/\tilde{F}_v)$ of the Galois character $\psi_{p,v}$ of F_v as above.

Let $\psi_{p,\tilde{w}} : \mathrm{Gal}(\tilde{E}_{\tilde{w}}^{\mathrm{ab}}/\tilde{E}_{\tilde{w}}) \rightarrow \mathcal{O}_{K,p}^\times$ be the continuous abelian character such that

$$\epsilon_{\tilde{w}}(x) = \psi_{p,\tilde{w}}(r_{\tilde{E}_{\tilde{w}}}(x)) \cdot N_\Phi(\mathrm{Nm}_{\tilde{E}_{\tilde{w}}/E_w}(x)) \quad (4)$$

for all $x \in \tilde{E}_{\tilde{w}}^\times$. To see that this makes sense, we have to check that the continuous homomorphism

$$\epsilon_{\tilde{w}} \cdot (N_\Phi \circ \mathrm{Nm}_{\tilde{E}_{\tilde{w}}/E_w})^{-1} : \tilde{E}_{\tilde{w}}^\times \rightarrow K_p^\times$$

has image contained in $\mathcal{O}_{K,p}^\times$ (and so it is of ‘‘Galois type’’: it factors through the profinite completion of its source). This is a problem of analyzing the image of a single uniformizer $\pi_{\tilde{w}}$ up to $\mathcal{O}_{K,p}^\times$ -multiple. Thus, it suffices to check that the product $\mathrm{Fr}_{B,q} \cdot N_\Phi(\pi_w)^{-[\kappa_{\tilde{w}}:\kappa_w]}$ in K_p^\times lies in $\mathcal{O}_{K,p}^\times$ for some uniformizer π_w in E_w . It suffices to check this after raising to the $[\kappa_v : \kappa_{\tilde{w}}]$ -th-power. Since $\kappa_{\tilde{w}} = \kappa_{w'} = \mathbb{F}_q$, the desired result follows from the fact that $\epsilon_v(\pi_v)$ is equal to $\mathrm{Fr}_{B,q}^{[\kappa_v:\kappa_{w'}]}$ and is an $\mathcal{O}_{K,p}^\times$ -multiple of $N_\Phi(\pi_w^{[\kappa_v:\kappa_w]})$ (due to the Galois character $\psi_{p,v}$ taking values in $\mathcal{O}_{K,p}^\times$).

By using Lemma 6.1(iv), we get the identity

$$(\psi_{p,v} \circ r_{F_v}) \circ \mathrm{Nm}_{\tilde{F}_v/F_v} = (\psi_{p,\tilde{w}} \circ r_{\tilde{E}_{\tilde{w}}}) \circ \mathrm{Nm}_{\tilde{F}_v/\tilde{E}_{\tilde{w}}}.$$

Thus, the character $\psi_{p,\tilde{w}}$ defines a descent G' over $\tilde{E}_{\tilde{w}}$ of the generic fiber G_1 of \mathcal{G}_1 over \tilde{F}_v equipped with its natural $\mathcal{O}_{K,p}$ -action. The p -divisible group G' over $\tilde{E}_{\tilde{w}}$ acquires ‘‘good reduction’’ over the finite unramified extension \tilde{F}_v in the sense that $G'_{\tilde{F}_v} \simeq G_1$ extends to the p -divisible group \mathcal{G}_1 over $\mathcal{O}_{\tilde{F}_v}$. The Galois descent data relative to $\tilde{F}_v/\tilde{E}_{\tilde{w}}$ on the generic fiber over \tilde{F}_v uniquely extends to \mathcal{G}_1 by Tate’s full faithfulness theorem [28], and since this extension is unramified we can use the equivalence of Galois descent and finite étale descent [5, 6.2B] at each torsion level over $\mathcal{O}_{\tilde{E}_{\tilde{w}}}$ to construct a unique p -divisible group \mathcal{G}' over $\mathcal{O}_{\tilde{E}_{\tilde{w}}}$ having generic fiber G' compatibly with the descent data. Again using Tate’s theorem, the $\mathcal{O}_{K,p}$ -action on G' extends uniquely to one on \mathcal{G}' .

(6.2) Lemma *The q -Frobenius endomorphism of the reduction $G'_0 := \mathcal{G}'_{\kappa_{\tilde{w}}}$ is given by the action of $\epsilon_{\tilde{w}}(\pi_{\tilde{w}}) \in \mathcal{O}_K$.*

This lemma (and the more general result in Proposition 6.3 below that we use in its proof) is a local version of Theorem 5.1(v) for p -divisible groups with complex multiplication.

PROOF. By decomposing G'_0 up to isogeny according to the factor fields of K_p , our task is a special case of the following problem. Let Γ be a p -divisible group of height d over a p -adic integer ring \mathcal{O}_F with finite residue field k of size q and fraction field F . Let L/\mathbb{Q}_p be an extension of degree d and assume that Γ is equipped with an action of L in the isogeny category over \mathcal{O}_F . Let $\mathbb{D}(\Gamma_0)$ denote the Dieudonné module of the special fiber Γ_0 of Γ , so $\mathbb{D}(\Gamma_0)[1/p]$ is a $W(k)[1/p] \otimes_{\mathbb{Q}_p} L$ -module that is necessarily invertible because the Frobenius automorphism of $\mathbb{D}(\Gamma_0)[1/p]$ is semilinear over the absolute Frobenius automorphism of $W(k)[1/p]$ (which in turn transitively permutes the factor fields of $W(k)[1/p] \otimes_{\mathbb{Q}_p} L$). Thus, the L -linear endomorphisms of $\mathbb{D}(\Gamma_0)[1/p]$ as a module over the Dieudonné ring are exactly the elements of L ; i.e., the reduction Γ_0 over k has L equal to its own centralizer in the endomorphism algebra of Γ_0 as a p -divisible group in the isogeny category over k . In particular, some nonzero element $\lambda \in L$ induces the q -Frobenius endomorphism of Γ_0 . We wish to compute λ in terms of the continuous Galois character $\psi : \text{Gal}(F^{\text{ab}}/F) \rightarrow \mathcal{O}_L^\times$ associated to the generic fiber Γ_F .

We claim that there is a unique homomorphism $\chi : F^\times \rightarrow L^\times$ that is algebraic with respect to \mathbb{Q}_p such that χ and $\psi \circ r_F : F^\times \rightarrow L^\times$ coincide on \mathcal{O}_F^\times and the resulting unramified character $(\psi \circ r_F) \cdot \chi^{-1} : F^\times \rightarrow L^\times$ carries uniformizers to λ . This certainly gives the desired result concerning G'_0 (due to (4), since $\epsilon_{\widehat{w}}$ is unramified), and it refines Serre's theory of locally algebraic representations since we are asserting algebraicity of $\psi \circ r_F$ on the entire local unit group. We wish to view this assertion as a special case of a general property of 1-dimensional abelian crystalline representations of p -adic fields (with coefficients in another p -adic field). To this end, we need to translate the hypotheses and desired conclusions into the context of p -adic Hodge theory.

Let $F_0 := W(k)[1/p]$ be the maximal unramified subfield of F . The representation ψ is crystalline since it is Barsotti–Tate, so $D_{\text{cris}}(\psi) = (\psi \otimes_{\mathbb{Q}_p} B_{\text{cris},F})^{\text{Gal}(\overline{F}/F)}$ is an invertible $L \otimes_{\mathbb{Q}_p} F_0$ -module equipped with a structure of L -linear filtered ϕ -module over F . By [11, 6.6] there is a natural F_0 -linear ϕ -compatible isomorphism

$$\eta_\Gamma : \text{Hom}_{F_0}(\mathbb{D}(\Gamma_0)[1/p], F_0) \simeq D_{\text{cris}}(\psi), \quad (5)$$

with ϕ acting Frobenius-semilinearly on the F_0 -linear dual of $\mathbb{D}(\Gamma_0)[1/p]$ in the usual manner (sending a functional f to $\sigma \circ f \circ \phi_{\mathbb{D}(\Gamma_0)}^{-1}$, where σ is the absolute Frobenius automorphism of F_0). Naturality forces η_Γ to be $L \otimes_{\mathbb{Q}_p} F_0$ -linear, so if $a = [k : \mathbb{F}_p]$ then $\sigma^a = \text{id}$ and the F_0 -linear ϕ^a on $D_{\text{cris}}(\psi)$ has to be multiplication by $1/\lambda$. Due to this inversion of λ , it remains to apply the general proposition below. \square

(6.3) Proposition *Let F and L be finite extensions of \mathbb{Q}_p , and let $r_F : F^\times \rightarrow \text{Gal}(F^{\text{ab}}/F)$ be the local Artin map with arithmetic normalization. Let $\psi : \text{Gal}(F^{\text{ab}}/F) \rightarrow \mathcal{O}_L^\times \subset L^\times$ be a continuous homomorphism. Let V be the $\mathbb{Q}_p[\text{Gal}(F^{\text{ab}}/F)]$ -module underlying a 1-dimensional L -vector space endowed with an L -linear action by $\text{Gal}(F^{\text{ab}}/F)$ via ψ .*

- (i) *The representation space V is crystalline if and only if there exists a homomorphism of \mathbb{Q}_p -groups*

$$\chi : \underline{F}^\times := \text{Res}_{F/\mathbb{Q}_p}(\mathbb{G}_m) \rightarrow \underline{K}^\times := \text{Res}_{K/\mathbb{Q}_p}(\mathbb{G}_m)$$

such that $\psi \circ r_F$ and χ (on \mathbb{Q}_p -points) coincide on \mathcal{O}_F^\times .

- (ii) *Assume that the condition in (i) is satisfied. Let $a = [\kappa_F : \mathbb{F}_p]$. The filtered ϕ -module $D_{\text{cris}}(V)$ over F covariantly attached to the crystalline representation V is free of rank 1 over $L \otimes_{\mathbb{Q}_p} F_0$ and its F_0 -linear endomorphism ϕ^a is given by the action of the product $\psi(r_F(\pi_F))^{-1} \cdot \chi(\pi_F) \in L^\times$, where $\pi_F \in \mathcal{O}_F$ is any uniformizer.*

PROOF. First assume that V is crystalline, so it is Hodge–Tate. The 1-dimensionality gives that V is semi-simple as a \mathbb{Q}_p -representation space of $\text{Gal}(\overline{F}/F)$, so it is also semisimple on the normal inertia subgroup. Hence, by [24, III, A.7] (and the initial hypotheses in [24, III, A.3]), $\psi|_{\text{Gal}(\overline{F}/F')}$ is locally algebraic for a finite extension F'/F in \overline{F} that splits L/\mathbb{Q}_p . That is, there is an algebraic map $\chi' : \underline{F}'^\times \rightarrow \underline{L}^\times$ such that χ' on \mathbb{Q}_p -points agrees with $\psi \circ r_F \circ \text{Nm}_{F'/F}$ near the identity in F'^\times . But $\text{Nm}_{F'/F} : \underline{F}'^\times \rightarrow \underline{F}^\times$ is a surjection of \mathbb{Q}_p -tori with connected kernel, so we may work on \mathbb{Q}_p -points near the identity to infer that χ' kills the torus $\ker(\text{Nm}_{F'/F})$. Hence, $\chi' = \chi \circ \text{Nm}_{F'/F}$ for a unique $\chi : \underline{F}^\times \rightarrow \underline{L}^\times$, and so $\psi \circ r_F$ and χ agree near the identity in F^\times ; in particular, ψ is locally algebraic. Obviously $\chi|_{\mathcal{O}_F^\times}$ can be extended to an \mathcal{O}_L^\times -valued Galois character θ_χ of F , and we claim that such a character is crystalline. (The choice of extension θ_χ does not matter, since the crystalline property only depends on the inertial restriction.) Assuming this property holds, then upon choosing θ_χ we get that $\psi \cdot \theta_\chi^{-1}$ is a crystalline representation of F with finite image on inertia. All such representations are unramified (e.g., due to the Dieudonné–Manin classification of isocrystals in the case of algebraically closed residue field). This would give that $\psi \circ r_F$ and χ coincide on \mathcal{O}_F^\times , assuming θ_χ is crystalline.

We see that to prove (i) it remains to show that for any algebraic homomorphism $\chi : \underline{F}^\times \rightarrow \underline{L}^\times$ over \mathbb{Q}_p , if its \mathcal{O}_F^\times -restriction on \mathbb{Q}_p -points is extended to an \mathcal{O}_L^\times -valued Galois character θ_χ of F then θ_χ is crystalline. This assertion is independent of the choice of θ_χ , since the crystalline property only depends on the inertial restriction. It is harmless to increase the scalar field L so that it splits F/\mathbb{Q}_p , so by the end of Remark 4.2 a basis of the \mathbb{Z} -module of such χ 's consists of the maps $[\tau] : \underline{F}^\times \rightarrow \underline{L}^\times$ induced on A -points by $\tau \otimes 1 : (F \otimes_{\mathbb{Q}_p} A)^\times \rightarrow (L \otimes_{\mathbb{Q}_p} A)^\times$ for all \mathbb{Q}_p -algebras A , where τ varies through the \mathbb{Q}_p -embeddings of F into L . It is therefore enough to treat the case $\chi = [\tau]^{-1}$ for some τ , in which case the \mathbb{Q}_p -representation space on inertia is the scalar extension by $\tau : F \rightarrow L$ of the inertial restriction of any Galois character $\psi : \text{Gal}(F^{\text{ab}}/F) \rightarrow \mathcal{O}_F^\times$ such that $(\psi \circ r_F)|_{\mathcal{O}_F^\times}$ is inversion. By [24, III, A.4] and our choice of the arithmetic normalization of local class field theory, examples of such Galois characters ψ are the Tate modules of Lubin–Tate formal groups, which arise from p -divisible groups and hence are crystalline. This proves (i).

As for (ii), we may increase L so that it splits F/\mathbb{Q}_p , and the proof of (i) shows that in such cases ψ is a product of \mathcal{O}_F^\times -valued Lubin–Tate characters (viewed with values in \mathcal{O}_L^\times via \mathbb{Q}_p -embeddings $\tau : F \rightarrow L$). The tensor-compatibility of D_{cris} (using the coefficient field L) and the multiplicativity of the proposed formula thereby reduces us to checking the special case when $L = F$ and ψ is the Lubin–Tate character $\text{Gal}(F^{\text{ab}}/F) \rightarrow \mathcal{O}_F^\times$ associated to a choice of uniformizer π_F . In this case $\psi(r_F(\pi_F)) = 1$ and the associated algebraic character $\chi : F^\times \rightarrow F^\times$ is inversion. Thus, by using the compatibility (5) of Dieudonné modules and D_{cris} , the inversions cancel out and we are reduced to checking that if G_{π_F} is the Lubin–Tate p -divisible group associated to π_F then its reduction over k has q_F -Frobenius endomorphism induced by π_F . This is the property that uniquely characterizes G_{π_F} . \square

Fix an isomorphism $\mathbb{F}_q \simeq \kappa_{\tilde{w}}$ so as to view B as an abelian variety over $\kappa_{\tilde{w}}$. The p -divisible groups $B[p^\infty]$ and G'_0 over $\kappa_{\tilde{w}}$ are endowed with actions by K_p in the isogeny category. Since $\alpha_B(\pi) = \text{Fr}_{B,q}$ and $\pi = \epsilon_{\tilde{w}}(\pi_{\tilde{w}})$, by Lemma 6.2 the element $\pi \in \mathcal{O}_K$ acts as the q -Frobenius endomorphism on each of these p -divisible groups. This is crucial in the proof of the following lemma.

(6.4) Lemma *There is an K_p -linear isogeny $B[p^\infty] \rightarrow G'_0$ over $\kappa_{\tilde{w}}$.*

PROOF. Let $k = \kappa_{\tilde{w}}$. We will use contravariant Dieudonné theory, so let $D_k = W(k)[\mathcal{F}, \mathcal{V}]$ denote the usual Dieudonné ring over the finite field k (non-commutative if $k \neq \mathbb{F}_p$). The category of $D_k[1/p]$ -modules that have finite dimension over $W(k)[1/p]$ and admit a D_k -stable $W(k)$ -lattice is anti-equivalent to the isogeny category of p -divisible groups over k . Note that the center of $D_k[1/p] = W(k)[1/p][\mathcal{F}]$ is $\mathbb{Q}_p[\mathcal{F}_q]$ where $\mathcal{F}_q = \mathcal{F}^{[k:\mathbb{F}_p]}$. The Dieudonné modules $\mathbb{D}(B[p^\infty])$ and $\mathbb{D}(G'_0)$ are D_k -modules that are finite free over $W(k)$ with rank $2g$ that is equal to the \mathbb{Z}_p -rank of $\mathcal{O}_{K,p}$, and each admits a D_k -linear action by $\mathcal{O}_{K,p}$. Thus, the underlying $W(k) \otimes_{\mathbb{Z}_p} \mathcal{O}_{K,p}$ -modules are invertible, due to the semilinearity of the \mathcal{F} -action over the absolute Frobenius automorphism of $W(k)$ and the faithfulness of the $\mathcal{O}_{K,p}$ -action on each p -divisible group. (For $B[p^\infty]$ the faithfulness of the $\mathcal{O}_{K,p}$ -action is due to the easier injectivity part of Tate's isogeny theorem for abelian varieties over finite fields, and for G'_0 the faithfulness can be checked after the ground field extension $\kappa_{\tilde{w}}/k$, where it becomes the p -divisible group of the reduction of the CM abelian variety (A_1, α_1) over $\tilde{F}_{\tilde{w}}$.)

Let $Z = \mathbb{Q}(\pi)$, so if $f \in \mathbb{Q}[T]$ is the minimal polynomial of π then $\mathbb{Q}[T]/(f) \simeq Z$ via $T \mapsto \pi$. Let $\prod_{v'|p} f_{v'}$ be its monic irreducible factorization in $\mathbb{Q}_p[T]$, corresponding to the decomposition $Z_p \simeq \prod_{v'|p} Z_{v'}$. Here, $Z_{v'} \simeq \mathbb{Q}_p[T]/(f_{v'})$ in which $\pi \in Z \subseteq Z_{v'}$ is the image of T . Since \mathcal{F}_q is central in $D_k[1/p]$, it makes sense to form the $Z_{v'}$ -algebra $C_{v'} = D_k[1/p]/D_k[1/p]f_{v'}(\mathcal{F}_q)$ in which the element $\pi \in Z_{v'}$ acts as \mathcal{F}_q . By the non-commutative algebra underlying the proof of the p -part of Tate's isogeny theorem for abelian varieties over finite fields (see [21] or [10, Thm. 8.4]), $C_{v'}$ is a central simple $Z_{v'}$ -algebra. Thus, the isomorphism class of a finitely generated left $C_{v'}$ -module is determined by its $Z_{v'}$ -dimension. Both $\mathbb{D}(B[p^\infty])[1/p]$ and $\mathbb{D}(G'_0)[1/p]$ are invertible modules over $W(k) \otimes_{\mathbb{Z}_p} K_p$, and the key point is that their $Z_{v'}$ -factors are left $C_{v'}$ -modules because the q -Frobenius endomorphisms of $B[p^\infty]$ and G'_0 are induced by the element $\pi \in \mathcal{O}_Z \subseteq \mathcal{O}_K$ whose image in $Z_{v'}$ is a root of $f_{v'} \in \mathbb{Q}_p[T]$. When viewing these Dieudonné modules as left $C_{v'}$ -modules, they have the same $Z_{v'}$ -dimension, namely that of the $Z_{v'}$ -part of the \mathbb{Z}_p -algebra $W(k) \otimes_{\mathbb{Z}_p} K_p$. Hence, the $Z_{v'}$ -factors are isomorphic as $C_{v'}$ -modules, and putting these together over all v' gives an \mathbb{Z}_p -linear isomorphism of the underlying $D_k[1/p]$ -modules. This provides a \mathbb{Z}_p -linear isogeny $B[p^\infty] \rightarrow G'_0$ over k , but it may not be K_p -linear. Hence, the resulting isomorphism of endomorphism algebras

$$\mathrm{End}^0(B[p^\infty]) \simeq \mathrm{End}^0(G'_0)$$

is \mathbb{Z}_p -linear but perhaps not K_p -linear.

These \mathbb{Z}_p -isomorphic endomorphism algebras are central simple \mathbb{Z}_p -algebras with the copy of K_p in each as a maximal commutative subalgebra because Tate's isogeny theorem gives $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{End}^0(B) \simeq \mathrm{End}^0(B[p^\infty])$ with $\mathrm{End}^0(B)$ a central simple Z -algebra having K as a maximal commutative Z -subalgebra. Hence, the Skolem–Noether theorem ensures that if we compose a choice of \mathbb{Z}_p -linear isogeny $B[p^\infty] \rightarrow G'_0$ with a suitable \mathbb{Z}_p -linear self-isogeny of G'_0 then we get a K_p -linear isogeny. \square

Using Lemma 6.4, we may choose a K_p -linear $\kappa_{\tilde{w}}$ -isogeny $B[p^\infty] \rightarrow G'_0$. The kernel is identified with a finite subgroup scheme of B over $\kappa_{\tilde{w}} = \mathbb{F}_q$, so if we replace B with its quotient modulo this kernel then we gain the property that there is a K_p -linear isomorphism $B[p^\infty] \simeq G'_0$ of p -divisible groups (not just an isogeny). To summarize, the p -divisible group \mathcal{G}' over $\mathcal{O}_{\tilde{E}_{\tilde{w}}}$ equipped with its K -action (in the isogeny category) is identified with a deformation of the p -divisible group of the abelian variety B over $\kappa_{\tilde{w}}$ equipped with its K -action (in the isogeny category). Hence, by working with CM orders we deduce via the Serre–Tate deformation theorem [15, 1.2.1] that there is a unique formal abelian scheme \mathfrak{A}' over $\mathrm{Spf}(\mathcal{O}_{\tilde{E}_{\tilde{w}}})$

equipped with an action of K (in the isogeny category) that compatibly deforms B and has p -divisible group \mathcal{G}' (respecting the K -actions). But the tangent space of \mathfrak{A}' coincides with that of \mathcal{G}' over $\mathcal{O}_{\tilde{E}_{\tilde{w}}}$, which in turn descends the tangent space $T_0(\mathcal{G}_1) \simeq T_0(\mathcal{A}_1)$ over $\mathcal{O}_{\tilde{F}_{\tilde{v}}}$, all respecting the actions by an order in \mathcal{O}_K . After inverting p this recovers $T_0(\mathcal{A}_1)_{\tilde{F}_{\tilde{v}}}$, on which the action of K is given by the p -adic CM-type Φ of $(A_1, \alpha_1)_{F_v}$. Hence, by Theorem 2.3, \mathfrak{A}' algebraizes to an abelian scheme \mathcal{A}' over $\mathcal{O}_{\tilde{E}_{\tilde{w}}}$ endowed with an action by K (in the isogeny category) giving rise to the CM-type Φ . This algebraization has reduction B and its p -divisible group is the descent \mathcal{G}' of $\mathcal{G}_1 = \mathcal{A}_1[p^\infty]$ compatibly with K -actions and the residual isomorphism $B[p^\infty] \simeq G'_0$.

Let (A', α') be the CM generic fiber of \mathcal{A}' over $\tilde{E}_{\tilde{w}}$ with its K -action, so it has good reduction that is K -linearly isomorphic to (B, α_B) over the initial choice of isomorphism $\kappa_{\tilde{w}} \simeq \mathbb{F}_q$ and its p -adic CM type is Φ . We have shown that (B, α_B) satisfies (NI) using the p -adic CM-type Φ on K and lifting over the integer ring of the subfield $\tilde{E}_{\tilde{w}} \subseteq \overline{\mathbb{Q}_p}$. This is a local version of Proposition 5.4, using $\tilde{E}_{\tilde{w}}$ rather than a number field. To complete the proof of Proposition 5.4, it remains to carry out one global step: descend (A', α') to a number field within $\tilde{E}_{\tilde{w}}$ (necessarily containing the reflex field $E \subseteq \overline{\mathbb{Q}_p}$ of the CM-type (K, Φ)); we can then increase such a number field within $\tilde{E}_{\tilde{w}}$ so that its completion at the place induced by \tilde{w} is $\tilde{E}_{\tilde{w}}$; in particular, this place has residue field $\kappa_{\tilde{w}}$ and the descent of A' has good reduction at this place. The required descent to a number field is given by the next lemma.

(6.5) Lemma *Any CM abelian variety X with good reduction over a p -adic field L descends to a CM abelian variety over a number field within L .*

PROOF. Fix a positive integer $n \geq 3$ not divisible by p , and let \mathcal{X} over $R = \mathcal{O}_L$ be the Néron model of X . The finite étale group scheme $\mathcal{X}[n]$ over R is uniquely determined by its special fiber. Let $F \subseteq L$ be a dense subfield that is a number field and let v be the induced p -adic place of F , so $F_v = L$. The special fiber of $\mathcal{X}[n]$ can be uniquely lifted to a finite étale group scheme \mathcal{G} over the henselization $\mathcal{O}_{F,(v)}^h$ of the algebraic local ring of \mathcal{O}_F at v , and by uniqueness of finite étale liftings over henselian local rings this descends $\mathcal{X}[n]$ via the canonical local inclusion $\mathcal{O}_{F,(v)}^h \rightarrow R$. The generic fiber of \mathcal{G} lives over an algebraic extension of \mathbb{Q} , so it descends to a finite étale group G over a number field $F' \subseteq L$.

We may choose an L -polarization of X , say with degree d^2 . Let $g = \dim(X)$, and let \mathcal{O} denote the CM order on X over L . Consider the moduli scheme M of finite type over F' classifying isomorphism classes of polarized abelian schemes of relative dimension g (over F' -schemes) endowed with the following extra structure: a degree- d^2 polarization, an isomorphism of the n -torsion with the pullback of the F' -group G , and a CM-structure by \mathcal{O} . Every geometric point of this moduli scheme M descends to $\overline{\mathbb{Q}}$, so M is 0-dimensional. Hence, the map $\text{Spec}(L) \rightarrow M$ corresponding to X with its additional structure factors through some point of M that is necessarily defined over a finite extension of F' . This is a number field within L to which X with its CM-structure descends. \square

§7. Open problems

In addition to the open problems raised in Remark 3.7(ii) and at the end of §3.6, here are two additional open questions concerning the lifting problems in §1.2.

(7.1) *Lifting.* Does (I) always hold? That is, is it true that any abelian variety over a finite field can be CM-lifted after possibly after applying an isogeny but not increasing the finite field?

(7.2) *Counterexample to (R).* In [23] it is shown that there exist examples of an abelian variety over $\overline{\mathbb{F}}_p$ which does not admit a CM lifting. Hence there exist examples of an abelian variety over a finite field for which (R) does not hold. Can we give an explicit example?

§A. Algebraic proof of Theorem 5.2

Due to lack of a suitable reference, in this appendix we provide a purely algebraic proof of Theorem 5.2 in modern terms. The reader is referred to the main text for the statement of this theorem (whose notation and hypotheses we shall use below without comment), as well as for an alternative reference for a proof in a different style.

First we check the uniqueness of (A, α) up to K -linear isogenies. If (A, α) and (A', α') are two such pairs, then since they have the same CM-type (K, Φ) there is a K -linear \mathbb{Q} -isogeny h between $A_{\overline{\mathbb{Q}}}$ and $A'_{\overline{\mathbb{Q}}}$. The invertible K_ℓ -modules $V_\ell(A)$ and $V_\ell(A')$ have $\text{Gal}(\overline{\mathbb{Q}}/F)$ acting through the same K_ℓ^\times -valued character (namely the continuous ψ_ℓ that is uniquely attached to ϵ), so all K_ℓ -linear maps $V_\ell(A) \rightarrow V_\ell(A')$ are automatically $\text{Gal}(\overline{\mathbb{Q}}/F)$ -equivariant. Thus, for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F)$ we have $V_\ell(\sigma^*(h)) = \rho_{A', \ell}(\sigma) \circ V_\ell(h) \circ \rho_{A, \ell}(\sigma)^{-1} = V_\ell(h)$, so $\sigma^*(h) = h$. That is, h is defined over F (and its F -descent is a K -linear isogeny). For existence, we will use Galois descent.

Step 1. By the classical theory of complex multiplication, there is a finite extension F'/F inside of $\overline{\mathbb{Q}}$ and a CM abelian variety (A', α') over F' with CM-type (K, Φ) . Its associated algebraic Hecke character $\epsilon' : \mathbb{A}_{F'}^\times \rightarrow K^\times$ has algebraic part $N_\Phi \circ \text{Nm}_{F'/E} = \epsilon_{\text{alg}} \circ \text{Nm}_{F'/F}$. Thus, the algebraic Hecke characters ϵ' and $\epsilon \circ \text{Nm}_{F'/F}$ have the same algebraic part. It follows from Remark 4.6(ii) that they are related through multiplication by a finite-order Hecke character of F' , so upon replacing F' with a finite extension we can arrange that $\epsilon' = \epsilon \circ \text{Nm}_{F'/F}$. We may and do also assume that F'/F is Galois. By means of a suitable F' -isogeny we can arrange that \mathcal{O}_K is the CM order (i.e., \mathcal{O}_K acts on A' as an abelian variety, not only in the isogeny category). We shall construct an \mathcal{O}_K -linear descent datum on $(A', \alpha')_{\overline{\mathbb{Q}}}$ with respect to $\overline{\mathbb{Q}}/F$, and the resulting F -descent (A, α) of $(A', \alpha')_{\overline{\mathbb{Q}}}$ will then be checked to have associated algebraic Hecke character ϵ ; it necessarily has CM type (K, Φ) .

For any finite idele $\xi \in \mathbb{A}_{K, f}^\times$, let $[\xi]_K$ denote the associated fractional ideal of \mathcal{O}_K . In particular, if $s \in \mathbb{A}_{E, f}^\times$ then the reflex norm $N_\Phi : \text{Res}_{E/\mathbb{Q}}(\mathbb{G}_m) \rightarrow \text{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$ yields a fractional ideal $[N_\Phi(s)]_K$. Recall also that if X is any \mathcal{O}_K -module scheme over a base scheme S and if M is any finite flat \mathcal{O}_K -module then there is an associated \mathcal{O}_K -module scheme $M \otimes_{\mathcal{O}_K} X$ over S that represents the functor $S' \rightsquigarrow M \otimes_{\mathcal{O}_K} X(S')$ on the category of S -schemes. In the special case that M is invertible and X is an abelian scheme with constant relative dimension g then $M \otimes_{\mathcal{O}_K} X$ is another such abelian scheme; if X with its \mathcal{O}_K -action is a CM abelian variety over a field of characteristic 0 then $M \otimes_{\mathcal{O}_K} X$ is another such (for invertible M) and it has the same CM type. This tensoring operation arises in one of the formulations of the Main Theorem of complex multiplication in its adelic form for CM abelian varieties with maximal CM order (see Theorem 5.2 in [6]), as follows.

Choose $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/E)$ and $s \in \mathbb{A}_{E, f}^\times$ satisfying $r_E(s) = \sigma|_{E^{\text{ab}}}$, and let I_s denote the fractional ideal $[N_\Phi(1/s)]_K$, so for all $n \geq 1$ the finite idele $N_\Phi(1/s) \in \mathbb{A}_{K, f}^\times$ gives a canonical

generator of the $\mathcal{O}_K/(n)$ -module I_s/nI_s . Then there is a unique K -linear $\overline{\mathbb{Q}}$ -isomorphism of abelian varieties

$$\theta_{\sigma,s} : [\mathbb{N}_\Phi(1/s)]_K \otimes_{\mathcal{O}_K} A'_\mathbb{Q} = I_s \otimes_{\mathcal{O}_K} A'_\mathbb{Q} \simeq (A'_\mathbb{Q})^\sigma$$

such that for all $n \geq 1$ the natural isomorphism $[\sigma] : A'_\mathbb{Q}[n](\overline{\mathbb{Q}}) \simeq (A'_\mathbb{Q})^\sigma[n](\overline{\mathbb{Q}})$ is given by the composite

$$A'_\mathbb{Q}[n](\overline{\mathbb{Q}}) \xrightarrow[\simeq]{\mathbb{N}_\Phi(1/s)} (I_s/nI_s) \otimes_{\mathcal{O}_K} A'_\mathbb{Q}[n](\overline{\mathbb{Q}}) \xrightarrow[\simeq]{} (I_s \otimes_{\mathcal{O}_K} A'_\mathbb{Q})[n](\overline{\mathbb{Q}}) \xrightarrow[\simeq]{\theta_{\sigma,s}} (A'_\mathbb{Q})^\sigma[n](\overline{\mathbb{Q}})$$

By uniqueness, for any $c \in E^\times$ we have that $\theta_{\sigma,cs}$ is the composition of $\theta_{\sigma,s}$ and the natural multiplication map by $\mathbb{N}_\Phi(c) \in K^\times$ carrying $I_{cs} = [\mathbb{N}_\Phi(1/(cs))]_K$ isomorphically to $I_s = [\mathbb{N}_\Phi(1/s)]_K$ as fractional ideals of \mathcal{O}_K . The intervention of $\mathbb{N}_\Phi(1/s)$ rather than $\mathbb{N}_\Phi(s)$ in the definition of $\theta_{\sigma,s}$ is due to the use of the arithmetic normalization of the Artin map (implicit in the requirement $r_E(s) = \sigma|_{E^{\text{ab}}}$). We are interested in applying this with $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F) \subseteq \text{Gal}(\overline{\mathbb{Q}}/E)$ and $s = \text{Nm}_{F/E}(\xi)$ for any $\xi \in \mathbb{A}_{F,f}^\times$ such that $r_F(\xi) = \sigma|_{F^{\text{ab}}}$ (so $r_E(s) = \sigma|_{E^{\text{ab}}}$).

Step 2. The key point is that if $\xi \in \mathbb{A}_{F,f}^\times$ then $[\mathbb{N}_\Phi(\text{Nm}_{F/E}(\xi))]_K$ is the principal fractional ideal generated by $\epsilon(\xi) \in K^\times$. To prove this, first recall that $\mathbb{N}_\Phi \circ \text{Nm}_{F/E} = \epsilon_{\text{alg}}$. Thus, it suffices to prove more generally that if L is a number field and $\chi : \mathbb{A}_L^\times \rightarrow L'^\times$ is an algebraic Hecke character valued in the multiplicative group of some number field L' then $\chi(s)$ is a generator of the fractional ideal $[(\chi_{\text{alg}})_\mathbb{A}(s)]_{L'}$, where $(\chi_{\text{alg}})_\mathbb{A} : \mathbb{A}_L^\times \rightarrow \mathbb{A}_{L'}^\times$ is the map induced by $\chi_{\text{alg}} : \text{Res}_{L/\mathbb{Q}}(\mathbb{G}_m) \rightarrow \text{Res}_{L'/\mathbb{Q}}(\mathbb{G}_m)$ on \mathbb{A} -points. Note that χ annihilates the infinitely divisible identity component of the archimedean factor L_∞^\times , and $(\chi_{\text{alg}})_\mathbb{A} \cdot \chi^{-1}$ may be viewed as a continuous homomorphism $\mathbb{A}_L^\times/L^\times \rightarrow \mathbb{A}_{L'}^\times$. In particular, it carries the compact norm-1 idele class group of L into the maximal compact subgroup of $\mathbb{A}_{L'}^\times$. But composing this map with projection to $\mathbb{A}_{L',f}^\times$ kills the image of the identity component of the archimedean factor L_∞^\times and so carries $\mathbb{A}_{L,f}^\times$ into the maximal compact subgroup $\prod_{v \nmid \infty} \mathcal{O}_{L',v}^\times$ (since any finite idele of L can be realized as the finite part of a norm-1 idele of L whose archimedean factor is in the identity component). This says that $[(\chi_{\text{alg}})_\mathbb{A}(s)]_{L'} = \chi(s)\mathcal{O}_{L'}$ as fractional ideals of $\mathcal{O}_{L'}$ for any $s \in \mathbb{A}_{L,f}^\times$, as desired.

For $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F) \subseteq \text{Gal}(\overline{\mathbb{Q}}/E)$, choose $\xi_\sigma \in \mathbb{A}_{F,f}^\times$ such that $\sigma|_{F^{\text{ab}}} = r_F(\xi_\sigma)$ in $\text{Gal}(F^{\text{ab}}/F)$ and let $s_\sigma = \text{Nm}_{F/E}(\xi_\sigma) \in \mathbb{A}_{E,f}^\times$. Thus, $[\mathbb{N}_\Phi(s_\sigma)]_K = [(\epsilon_{\text{alg}})_\mathbb{A}(\xi_\sigma)]_K = \epsilon(\xi_\sigma)\mathcal{O}_K$, so we have a K -linear isomorphism

$$A'_\mathbb{Q} \xrightarrow[\simeq]{\epsilon(\xi_\sigma)^{-1}} [\mathbb{N}_\Phi(1/s_\sigma)]_K \otimes_{\mathcal{O}_K} A'_\mathbb{Q} \xrightarrow[\simeq]{\theta_{\sigma,s_\sigma}} (A'_\mathbb{Q})^\sigma.$$

We shall prove that this is independent of the choice of ξ_σ and defines a Galois descent datum on $(A', \alpha')_{\overline{\mathbb{Q}}}$ with respect to $\text{Gal}(\overline{\mathbb{Q}}/F)$ such that the resulting descent (A, α) over F is the desired CM abelian variety. To prove the independence of the choice of ξ_σ , suppose that $\xi'_\sigma \in \mathbb{A}_{F,f}^\times$ is another such choice, so $\xi'_\sigma \xi_\sigma^{-1} \in \ker r_F = F_\infty^\times F^\times$. Thus, the element $\xi'_\sigma \xi_\sigma^{-1} \in \mathbb{A}_{F,f}^\times \simeq \mathbb{A}_F^\times/F_\infty^\times$ is in the closure of F^\times in $\mathbb{A}_{F,f}^\times$, so for any open subset $U \subseteq \mathbb{A}_{F,f}^\times$ around the identity there exists $\lambda \in F^\times$ such that $\xi'_\sigma \in \lambda \xi_\sigma U$. Since $\ker \epsilon$ meets $\mathbb{A}_{F,f}^\times$ in an open subgroup and $[\mathbb{N}_\Phi(s_\sigma)]_K$ only depends on s_σ modulo the maximal compact open subgroup in $\mathbb{A}_{E,f}^\times$, it suffices to check two things: (a) if $\xi'_\sigma = \lambda \xi_\sigma$ for some $\lambda \in F^\times$ then we get the same composite isomorphism $A'_\mathbb{Q} \simeq (A'_\mathbb{Q})^\sigma$ in both cases, and (b) for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/E)$ and $s \in \mathbb{A}_{E,f}^\times$ such that $r_E(s) = \sigma|_{E^{\text{ab}}}$, the isomorphism $\theta_{\sigma,s}$ is unaffected by replacing s with us for $u \in \mathbb{A}_{E,f}^\times \cap \ker r_E$ sufficiently near the identity (perhaps depending on s).

In case (a), $s'_\sigma := \text{Nm}_{F/E}(\xi'_\sigma)$ is equal to $\text{Nm}_{F/E}(\lambda) \cdot s_\sigma$, so $\text{N}_\Phi(s'_\sigma) = \epsilon(\lambda)\text{N}_\Phi(s_\sigma)$. The required equality of $\overline{\mathbb{Q}}$ -isomorphisms $A'_{\overline{\mathbb{Q}}} \simeq (A'_\mathbb{Q})^\sigma$ in this case therefore reduces to the general identity relating $\theta_{\sigma,s}$ and $\theta_{\sigma,cs}$ via the action of $\text{N}_\Phi(c) \in K^\times$ for any $c \in E^\times$ (such as $c = \text{Nm}_{F/E}(\lambda)$). Meanwhile, to study the general behavior of $\theta_{\sigma,s}$ under multiplication of s against any $u \in (\ker r_E) \cap \mathbb{A}_{E,f}^\times$ that is sufficiently near to the identity, we can restrict our attention to multiplication by $u \in (\ker r_E) \cap \prod_{v \nmid \infty} \mathcal{O}_{E,v}^\times$. If $s' = us$ for such a u then $[\text{N}_\Phi(s')]_K = [\text{N}_\Phi(s)]_K$, so $\theta_{\sigma,s}^{-1} \circ \theta_{\sigma,s'}$ is an automorphism of $[\text{N}_\Phi(1/s)]_K \otimes_{\mathcal{O}_K} A'_\mathbb{Q}$. Moreover, by taking u sufficiently near to 1 we can ensure that $\theta_{\sigma,s}$ and $\theta_{\sigma,s'}$ induce the same map on m -torsion for a fixed $m \geq 3$, so $\theta_{\sigma,s}^{-1} \circ \theta_{\sigma,s'}$ is trivial on the m -torsion. If we choose a K -linear polarization ϕ of $A'_\mathbb{Q}$ then it follows from Lemma 5.1 in [6] and the subsequent construction of $\theta_{\sigma,s}$ in loc. cit. that $\theta_{\sigma,s}^{-1} \circ \theta_{\sigma,s'}$ commutes with a polarization $\phi_s = \phi_{s'}$ canonically associated to ϕ and the fractional ideal $[\text{N}_\Phi(s)]_K = [\text{N}_\Phi(s')]_K$. But an automorphism of a polarized abelian variety has finite order and hence is trivial when it is trivial on the m -torsion for some $m \geq 3$.

This completes the verification that the choice of ξ_σ as above does not matter, so we have constructed a canonical K -linear $\overline{\mathbb{Q}}$ -isomorphism

$$c(\sigma) : A'_{\overline{\mathbb{Q}}} \simeq (A'_\mathbb{Q})^\sigma$$

for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F)$.

Step 3. Since the isomorphisms $\theta_{\sigma,s}$ are K -linear and we can use $\xi_\sigma \xi_\tau$ as $\xi_{\sigma\tau}$, it is easy to check that the cocycle relation $c(\sigma\tau) \stackrel{?}{=} \sigma^*(c(\sigma)) \circ c(\tau)$ for $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/F)$ reduces to the general identity $\theta_{\sigma\tau, st} \stackrel{?}{=} \sigma^*(\theta_{\tau,t}) \circ (1 \otimes \theta_{\sigma,s})$ as isomorphisms

$$[\text{N}_\Phi(1/st)]_K \otimes_{\mathcal{O}_K} A'_\mathbb{Q} \simeq [\text{N}_\Phi(1/t)]_K \otimes_{\mathcal{O}_K} ([\text{N}_\Phi(1/s)]_K \otimes_{\mathcal{O}_K} A'_\mathbb{Q}) \rightrightarrows ((A'_\mathbb{Q})^\tau)^\sigma \simeq (A'_\mathbb{Q})^{\sigma\tau}$$

for $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/E)$ and $s, t \in \mathbb{A}_{E,f}^\times$ such that $r_E(s) = \sigma|_{E^{\text{ab}}}$ and $r_E(t) = \tau|_{E^{\text{ab}}}$. This identity is immediately deduced from the unique characterization of $\theta_{\sigma\tau, st}$.

To carry out the descent, we require a continuity condition on $\sigma \mapsto c(\sigma)$ as follows. By the construction of $\theta_{\sigma,s} : [\text{N}_\Phi(1/s)]_K \otimes_{\mathcal{O}_K} A'_\mathbb{Q} \simeq (A'_\mathbb{Q})^\sigma$ in §4–§5 of [6], there is a finite extension L/F' inside of $\overline{\mathbb{Q}}$ that is Galois over F such that $\theta_{\sigma,s}$ descends to a (necessarily K -linear) L -isomorphism $[\text{N}_\Phi(1/s)]_K \otimes_{\mathcal{O}_K} A'_L \simeq (A'_L)^{\sigma|_L}$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/E)$ and $s \in \mathbb{A}_{E,f}^\times$ such that $r_E(s) = \sigma|_{E^{\text{ab}}}$. (We do not expect that we can take $L = F'$.) Hence, for every $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F)$ the isomorphism $c(\sigma)$ descends to a K -linear L -isomorphism $c_L(\sigma) : A'_L \simeq (A'_L)^{\sigma|_L}$. If we increase L to split $A'[m]$ for a fixed $m \geq 3$ then it follows that $c_L(\sigma)$ is the identity on m -torsion when $\sigma|_L$ is trivial. Moreover, upon choosing a K -linear F' -polarization ϕ of A' , with the help of the associated K -linear polarizations ϕ_α of $[\text{N}_\Phi(\alpha)]_K \otimes_{\mathcal{O}_K} A'$ constructed for all $\alpha \in \mathbb{A}_{E,f}^\times$ as in Lemma 5.1 of [6] we deduce that $c_L(\sigma)$ carries ϕ_L to $(\phi_L)^{\sigma|_L}$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F)$.

Hence, if $\sigma|_L$ is the identity then $c_L(\sigma)$ is an automorphism of a polarized abelian variety that is trivial on the m -torsion with some $m \geq 3$, so $c_L(\sigma)$ is the identity for such σ . It follows (using the cocycle relation) that $c_L(\sigma)$ only depends on $\sigma|_L$, so we can view c_L as a function on $\text{Gal}(L/F)$ that defines a K -linear Galois descent datum on A'_L with respect to L/F . In other words, if we rename L as F' (as we may), then we get to the case where

$$\sigma \mapsto c_{F'}(\sigma) \in \text{Isom}(A', A'^\sigma)$$

is a Galois descent datum on (A', α') with respect to F'/F . By descent theory, this uniquely determines an abelian variety A over F equipped with a ring homomorphism $\alpha : \mathcal{O}_K \rightarrow \text{End}(A)$ and a K -linear F' -isomorphism $A_{F'} \simeq A'$ respecting the Galois descent data on both sides.

Step 4. Let $\epsilon_A : \mathbb{A}_F^\times \rightarrow K^\times$ be the algebraic Hecke character associated to (A, α) . To prove that $\epsilon_A = \epsilon$, it suffices (by Lemma 4.9) to show that for a fixed choice of rational prime ℓ the continuous ℓ -adic characters $\psi_\ell, \psi'_\ell : \text{Gal}(F^{\text{ab}}/F) \rightarrow K_\ell^\times$ that are respectively uniquely associated to ϵ and ϵ_A coincide. By Theorem 5.1(ii), ψ'_ℓ computes the action of $\text{Gal}(F^{\text{ab}}/F)$ on $V_\ell(A)$. Also, by construction, $\psi_\ell(r_F(\xi)) = \epsilon(\xi)N_\Phi(\text{Nm}_{F/E}(1/\xi))_\ell$ for all $\xi \in \mathbb{A}_{F,f}^\times$. Thus, if we choose $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F)$ then we want σ to act on $V_\ell(A)$ as multiplication by $\epsilon(\xi_\sigma)N_\Phi(\text{Nm}_{F/E}(1/\xi_\sigma))_\ell$ for any $\xi_\sigma \in \mathbb{A}_{F,f}^\times$ such that $r_F(\xi_\sigma) = \sigma|_{F^{\text{ab}}}$.

Fix such a σ and ξ_σ , and let $s_\sigma = \text{Nm}_{F/E}(\xi_\sigma)$. It is evident that σ acting on $V_\ell(A)$ is the composition of two maps: the canonical σ -pullback map $[\sigma] : V_\ell(A_{\overline{\mathbb{Q}}}) \simeq V_\ell((A_{\overline{\mathbb{Q}}})^\sigma)$ and the isomorphism on ℓ -adic Tate spaces induced by the descent-data isomorphism $(A_{\overline{\mathbb{Q}}})^\sigma \simeq A_{\overline{\mathbb{Q}}}$. But the definition of A by $\text{Gal}(\overline{\mathbb{Q}}/F)$ -descent of $A'_{\overline{\mathbb{Q}}}$ with respect to the 1-cocycle $\sigma \mapsto c(\sigma)$ provides a canonical isomorphism $A_{\overline{\mathbb{Q}}} \simeq A'_{\overline{\mathbb{Q}}}$ with respect to which the first step, $[\sigma]$, is identified with the composition of $V_\ell(\theta_{\sigma, s_\sigma})$ and the isomorphism

$$V_\ell(A_{\overline{\mathbb{Q}}}) \simeq [N_\Phi(1/s_\sigma)]_K \otimes_{\mathcal{O}_K} V_\ell(A_{\overline{\mathbb{Q}}}) \simeq V_\ell([N_\Phi(1/s_\sigma)]_K \otimes_{\mathcal{O}_K} A_{\overline{\mathbb{Q}}})$$

induced by multiplication by the ℓ -part $N_\Phi(1/s_\sigma)_\ell$ of the finite idele $N_\Phi(1/s_\sigma) \in \mathbb{A}_{K,f}^\times$. Meanwhile, the descent data isomorphism $A_{\overline{\mathbb{Q}}} \simeq (A_{\overline{\mathbb{Q}}})^\sigma$ is (by definition in terms of $A'_{\overline{\mathbb{Q}}}$) identified with the composition of $\theta_{\sigma, s_\sigma}$ and the multiplication map induced by the principal generator $\epsilon(1/\xi_\sigma) \in K^\times$ of $[N_\Phi(1/s_\sigma)]_K$. Passing to the inverse of this latter composition, on ℓ -adic Tate spaces we recover the descent data isomorphism $V_\ell((A_{\overline{\mathbb{Q}}})^\sigma) \simeq V_\ell(A_{\overline{\mathbb{Q}}})$ that is the second step in the description of the σ -action on $V_\ell(A)$. Composing both steps, the two contributions from the mysterious $\theta_{\sigma, s_\sigma}$ cancel out and what remains is easily identified with the product of multiplication by $N_\Phi(1/s_\sigma)_\ell = N_\Phi(\text{Nm}_{F/E}(1/\xi_\sigma))_\ell \in K_\ell^\times$ and by $\epsilon(\xi_\sigma) \in K^\times$ on $V_\ell(A)$, exactly as desired.

References

- [1] Artin, E. and Tate, J. Class field theory. Advanced Book Classics, Addison-Wesley, New York, 1990.
- [2] Berthelot, P. and Breen, L. and Messing, W. Théorie de Dieudonné cristalline II. LNM 930, Springer-Verlag 1982.
- [3] Berthelot, P. and Ogus, A. F -isocrystals and de Rham cohomology I. Inv. Math. 72, 1983, 159–199.
- [4] Bosch, S. and Güntzer, U. and Remmert, R. Non-archimedean analysis. Grundlehren 261, Springer-Verlag, New York, 1983.
- [5] Bosch, S. and Lütkebohmert, W. and Raynaud, M. Néron models. Ergebnisse der Mathematik 21, Springer-Verlag, New York, 1990.
- [6] Conrad, B. Main Theorem of Complex Multiplication. In “Notes on complex multiplication”, available at www.math.stanford.edu/~conrad/.

- [7] 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.
- [8] Deligne, P. Motifs et groupes de Taniyama. In *Hodge Cycles, Motives, and Shimura Varieties*, LNM 900, Springer-Verlag, 1982, 261–279.
- [9] Dieudonné, J. and Grothendieck, A. Éléments de géométrie algébrique. Publ. Math. IHES 11, 1961.
- [10] Eisenträger, K. The Theorem of Honda and Tate. In “Notes on complex multiplication”, available at www.math.stanford.edu/~conrad/.
- [11] 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.
- [12] Hazewinkel, M. Formal groups and applications. Academic Press, New York, 1978.
- [13] Jacobson, N. Basic algebra II. W.H. Freeman & Co., 1989.
- [14] deJong, A.J. Crystalline Dieudonné module theory via formal and rigid geometry. Publ. Math. IHES 82, 1995, 5–96.
- [15] Katz, N.M. Serre–Tate local moduli. Springer LNM 868, 1981, 138–202.
- [16] Lang, S. *Complex Multiplication*. Grundlehren mathematischen Wissenschaften 255, Springer-Verlag, 1983.
- [17] Mazur, B. and Messing, W. Universal extensions and one-dimensional crystalline cohomology. Springer LNM 370, Springer-Verlag, 1974.
- [18] Messing, W. The crystals associated to Barsotti–Tate groups: with applications to abelian schemes. Springer LNM 264, Springer-Verlag, 1972.
- [19] 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.
- [20] Milne, J. and Shih, K.-Y. Langlands’ construction of the Taniyama group. In *Hodge Cycles, Motives, and Shimura Varieties*, LNM 900, Springer-Verlag, 1982, 229–260.
- [21] Milne, J. and 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.
- [22] 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.
- [23] Oort, F. CM-lifting of abelian varieties. *J. Alg. Geom.* 1, 1992, 131–146.
- [24] Serre, J.-P. *Abelian ℓ -Adic Representations and Elliptic Curves*. W. A. Benjamin, 1968.

- [25] Serre, J.-P. and Tate, J. Good reduction of abelian varieties. *Ann. Math.* 88, 1965, 492–517.
- [26] Shimura, G. and Taniyama, Y. *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*. Publ. Math. Soc. Japan, 6, 1961.
- [27] Tate, J. Endomorphisms of abelian varieties over finite fields. *Inv. Math.* 2, 1966, 134–144.
- [28] Tate, J. p -divisible groups. In *Proc. Conf. on Local Fields*, Springer-Verlag, 1967, 148–183.
- [29] 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.
- [30] 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.
- [31] Yu, C.-F. The isomorphism classes of abelian varieties of CM-type. *J. of Pure and Applied Algebra* 187, 2004, 305–319.