CHAPTER 1

Algebraic theory of complex multiplication

The theory of complex multiplication... is not only the most beautiful part of mathematics but also of all science.

— David Hilbert

1.1. Introduction

1.1.1. Lifting questions. A natural question early in the theory of abelian varieties is whether every abelian variety in positive characteristic admits a lift to characteristic 0. That is, given an abelian variety A_0 over a field κ with $\mathrm{char}(\kappa) > 0$, does there exist a local domain R of characteristic zero with residue field κ and an abelian scheme A over R whose special fiber A_κ is isomorphic to A_0? We may also wish to demand that a specified polarization of A_0 or subring of the endomorphism algebra of A_0 (or both) also lifts to A. (The functor $A \rightsquigarrow A_\kappa$ from abelian R-schemes to abelian varieties over κ is faithful, by consideration of finite étale torsion levels; see the beginning of 1.4.4.)

Suppose there is an affirmative solution A to such a lifting problem over some local domain R as above. Let's see that we can arrange for a solution to be found over a local *noetherian* domain (that is even complete). This rests on a direct limit technique (that is very useful throughout algebraic geometry), as follows. Observe that for the directed system of noetherian local subrings R_i with local inclusions $R_i \hookrightarrow R$, we have $R = \varinjlim R_i$. In [**34**, IV_3, §8–§12; IV_4, §17] there is an exhaustive development of the technique of descent through direct limits. The principle is that if $\{D_i\}$ is a directed system of rings with limit D, and if we are given a "finitely presented" algebro-geometric situation over D (a diagram of finitely many D-schemes of finite presentation, equipped with with finitely many D-morphisms among them and perhaps some finitely presented quasi-coherent sheaves on them, some of which may be D-flat, etc.) then the entire structure descends to D_i for sufficiently large i. Moreover, if we increase i enough then we can also descend "reasonable" properties (such as flatness for morphisms or sheaves, and properness, surjectivity, smoothness, and having geometrically connected fibers for morphisms), any two descents become isomorphic after increasing i some more, and so on.

The results of this direct limit formalism are intuitively plausible, but their proofs can be rather non-obvious to the uninitiated (e.g., descending the properties of flatness and surjectivity). We will often use this limit formalism without much explanation, and we hope that the plausibility of such results is sufficient for a non-expert reader to follow the ideas. Everything we need is completed proved in the cited sections of [**34**]. As a basic example, since the condition of being an abelian scheme amounts to a group scheme diagram for a smooth proper R-scheme having geometrically connected fibers, the abelian scheme A over R descends to an abelian scheme over R_{i_0} for some sufficiently large i_0.

The residue field κ_{i_0} of R_{i_0} is merely a subfield of κ. By [**34**, $0_{\rm III}$, 10.3.1], there is a faithfully flat local extension $R_{i_0} \to R'$ with R' *noetherian* and having residue field κ over κ_{i_0}. By faithful flatness, every minimal prime of $\widehat{R'}$ has residue characteristic 0, so we can replace $\widehat{R'}$ with its quotient by such a prime to obtain a solution over a *complete* local noetherian domain with residue field κ.

Typically our liftings will be equipped with additional structure such as a polarization, and so the existence of an affirmative solution for our lifting problem (for a given A_0) often amounts to an appropriate deformation ring $\mathcal{R}$ for A_0 (over a Cohen ring for κ) admitting a generic point in characteristic 0; the coordinate ring of the corresponding irreducible component of $\mathrm{Spec}(\mathcal{R})$ is such an R. If $\kappa \to \kappa'$ is an extension of fields and $W \to W'$ is the associated extension of Cohen rings then often there is a natural isomorphism $\mathcal{R}' \simeq W'\widehat{\otimes}_W \mathcal{R}$ relating the corresponding deformation rings for A_0 and $(A_0)_{\kappa'}$ (see 1.4.4.5, 1.4.4.13, and 1.4.4.14). Thus, if $\mathcal{R}'$ has a generic point of characteristic 0 then so does $\mathcal{R}$. Hence, to prove an affirmative answer to lifting questions as above it is usually enough to consider algebraically closed κ. For example, the general lifting problem for polarized abelian varieties (allowing polarizations for which the associated symmetric isogeny $A_0 \to A_0^t$ is not separable) was solved affirmatively by Norman-Oort [**85**, Cor. 3.2] when $\kappa = \overline{\kappa}$, and the general case follows by deformation theory (via 1.4.4.14 with $\mathcal{O} = \mathbb{Z}$).

1.1.2. Refinements. When a lifting problem as above has an affirmative solution, it is natural to ask if the (complete local noetherian) base ring R for the lifting can be chosen to satisfy nice ring-theoretic properties, such as being normal or a discrete valuation ring. Slicing methods allow one to find an R with $\dim(R) = 1$ (see 2.1.1 for this argument), but normalization generally increases the residue field. Hence, asking that the complete local noetherian domain R be normal or a discrete valuation ring with a specified residue field κ is a non-trivial condition unless κ is algebraically closed.

We are interested in versions of the lifting problem for finite κ when we lift not only the abelian variety but also a large commutative subring of its endomorphism algebra. To avoid counterexamples it is sometimes necessary to weaken the lifting problem by permitting the initial abelian variety A_0 to be replaced with another in the same isogeny class over κ. In 1.8 we will precisely formulate several such lifting problems involving complex multiplication, and the main result of our work is a rather satisfactory solution to these lifting problems.

1.1.3. Purpose of this chapter. Much of the literature on complex multiplication involves either (i) working over an algebraically closed ground field, (ii) making unspecified finite extensions of the ground field, or (iii) restricting attention to simple abelian varieties. To avoid any uncertainty about the degree of generality in which various foundational results in the theory are valid, as well as to provide a convenient reference for subsequent considerations, in this chapter we provide an extensive review of the algebraic theory of complex multiplication over a general base field. This includes special features of the theory over finite fields and over fields of characteristic 0, and for some important proofs we refer to the original literature (e.g., papers of Tate). Some arithmetic aspects (such as reflex fields and the Main Theorem of Complex Multiplication) are discussed in Chapter 2, and Appendix A provides proofs of the Main Theorem of Complex Multiplication and some results of Tate over finite fields.

1.2. Simplicity, isotypicity, and endomorphism algebras

1.2.1. Simple abelian varieties. An abelian variety A over a field K is *simple* (over K) if it is non-zero and contains no non-zero proper abelian subvarieties. Simplicity is not generally preserved under extension of the base field; see Example 1.6.3 for some two-dimensional examples over finite fields and over $\mathbb{Q}$. An abelian variety A over K is *absolutely simple* (over K) if $A_{\overline{K}}$ is simple.

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

Proof. This is an application of direct limit and specialization arguments, as we now explain. Assume for some K'/K that there is a non-zero proper abelian subvariety $B' \subset A_{K'}$. By replacing K' with an algebraic closure we may arrange that K' and then especially K is algebraically closed. (The algebraically closed property for K' is unimportant, but it is crucial that we have it for K.) By expressing K' as a direct limit of finitely generated K-subalgebras, there is a finitely generated K-subalgebra $R \subset K'$ such that $B' = B_{K'}$ for an abelian scheme $B \to \mathrm{Spec}(R)$ that is a closed R-subgroup of A_R.

The constant positive dimension of the fibers of $B \to \mathrm{Spec}(R)$ is strictly less than $\dim(A)$, as we may check using the K'-fiber $B' \subset A_{K'}$. Since K is algebraically closed we can choose a K-point x of $\mathrm{Spec}(R)$. The fiber B_x is a non-zero proper abelian subvariety of A, contrary to the simplicity of A over K. □

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

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

1.2.1.2. Lemma (Chow)**.** *Let K'/K be an extension of fields that is primary* (*i.e., K is separably algebraically closed in K'*)*. For abelian varieties A and B over K, the natural map* $\mathrm{Hom}(A, B) \to \mathrm{Hom}(A_{K'}, B_{K'})$ *is bijective.*

Proof. See [**23**, Thm. 3.19] for a proof using faithfully flat descent (which is reviewed at the beginning of [**23**, §3]). An alternative proof is to show that the locally finite type Hom-scheme $\underline{\mathrm{Hom}}(A, B)$ over K is étale. □

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

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

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

PROOF. When K is algebraically closed this result is proved in [**82**, §19, Thm. 1]. The same method works for perfect K, as explained in [**76**, Prop. 12.1]. (Perfectness is implicit in the property that the underlying reduced scheme of a finite type K-group is a K-subgroup. For a counterexample over any imperfect field, see [**25**, Ex. A.3.8].) The general case can be pulled down from the perfect closure via Lemma 1.2.1.2; see the proof of [**23**, Cor. 3.20] for the argument. □

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

PROOF. By the Poincaré reducibility theorem, abelian subvarieties of A are precisely the images of maps $A \to A$, and similarly for $A_{K'}$. Since scalar extension commutes with the formation of images, the assertion is reduced to the bijectivity of $\mathrm{End}(A) \to \mathrm{End}(A_{K'})$, which follows from Lemma 1.2.1.2. □

Since any map between simple abelian varieties over K is either 0 or an isogeny, by general categorical arguments the collection of C_i's (up to isogeny) in the Poincaré reducibility theorem is unique up to rearrangement, and the multiplicities e_i are also uniquely determined.

1.2.1.5. Definition. The C_i's in the Poincaré reducibility theorem (considered up to isogeny) are the *simple factors* of A.

By the uniqueness of the simple factors up to isogeny, we deduce:

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

1.2.2. Central simple algebras. Using notation from the Poincaré reducibility theorem, for a non-zero abelian variety A we have

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

where $\{C_i\}$ is the set of simple factors of A and the e_i's are the corresponding multiplicities. Each $\mathrm{End}^0(C_i)$ is a division algebra, by simplicity of the C_i's. Thus, to understand the structure of endomorphism algebras of abelian varieties we need to understand matrix algebras over division algebras, especially those of finite dimension over $\mathbb{Q}$. We therefore next review some general facts about such rings.

Although we have used K to denote the ground field for abelian varieties above, in what follows we will use K to denote the ground field for central simple algebras; the two are certainly not to be confused, since for abelian varieties in positive characteristic the endomorphism algebras are over fields of characteristic 0.

1.2.2.1. Definition. A *central simple algebra* over a field K is a non-zero associative K-algebra of finite dimension such that K is the center and the underlying ring is simple (i.e., has no non-trivial two-sided ideals).

A *central division algebra* over K is a central simple algebra over K whose underlying ring is a division algebra.

Among the most basic examples of central simple algebras over a field K are the matrix algebras $\mathrm{Mat}_n(K)$ for $n \geqslant 1$. The most general case is given by:

1.2.2.2. Proposition (Wedderburn's Theorem)**.** *Every central simple algebra D over a field K is isomorphic to $\mathrm{Mat}_n(\Delta) = \mathrm{End}_\Delta(\Delta^{\oplus n})$ for some $n \geqslant 1$ and some central division algebra Δ over K (where $\Delta^{\oplus n}$ is a left Δ-module). Moreover, n is uniquely determined by D, and Δ is uniquely determined up to K-isomorphism.*

Proof. This is a special case of a general structure theorem for simple rings; see [**53**, Thm. 4.2] and [**53**, §4.4, Lemma 2]. □

In addition to matrix algebras, another way to make new central simple algebras from old ones is to use tensor products:

1.2.2.3. Lemma. *If D and D' are central simple algebras over a field K, then so is $D \otimes_K D'$. For any extension field K'/K, $D_{K'} := K' \otimes_K D$ is a central simple K'-algebra.*

Proof. The first part is [**53**, §4.6, Cor. 3]; the second is [**53**, §4.6, Cor. 1, 2]. □

1.2.3. Splitting fields. It is a general fact that for any central division algebra Δ over a field K, Δ_{K_s} is a matrix algebra over K_s (so $[\Delta : K]$ is a square). In other words, Δ is split by a finite separable extension of K. There is a refined structure theory concerning splitting fields and maximal commutative subfields of central simple algebras over fields; [**53**, §4.1–4.6] gives a self-contained development of this material. An important result in this direction is:

1.2.3.1. Proposition. *Let D be a central simple algebra over a field F, with $[D : F] = n^2$. An extension field F'/F with degree n embeds as an F-subalgebra of D if and only if F' splits D (i.e., $D_{F'} \simeq \mathrm{Mat}_n(F')$). Moreover, if D is a division algebra then every maximal commutative subfield of D has degree n over F.*

Proof. The first assertion is a special case of [**53**, Thm. 4.12]. Now assume that D is a division algebra and consider a maximal commutative subfield F'. In such cases F' splits D (by [**53**, §4.6, Cor. to Thm. 4.8]), so $n|[F' : F]$ by [**53**, Thm. 4.12]. To establish the reverse divisibility it suffices to show that for *any* central simple algebra D of dimension n^2 over F, every commutative subfield of D has F-degree at most n. If A is any simple F-subalgebra of D and its centralizer in D is denoted $Z_D(A)$ then $n^2 = [A : F][Z_D(A) : F]$ by [**53**, §4.6, Thm. 4.11]. Thus, if A is also commutative (so A is contained in $Z_D(A)$) then $[A : F] \leqslant n$. □

The second assertion in Proposition 1.2.3.1 does not generalize to central simple algebras; e.g., perhaps $D = \mathrm{Mat}_n(F)$ with F having no degree-n extension fields.

In general, for a splitting field F'/F of a central simple F-algebra D, the choice of isomorphism $D_{F'} \simeq \mathrm{Mat}_n(F')$ is ambiguous up to composition with the action of $\mathrm{Aut}_{F'}(\mathrm{Mat}_n(F'))$, so it is useful to determine this automorphism group. The subgroup of *inner automorphisms* is $\mathrm{GL}_n(F')/F'^{\times}$, arising from conjugation against elements of $\mathrm{Mat}_n(F')^{\times} = \mathrm{GL}_n(F')$. In general, the inner automorphisms are the only ones:

1.2.3.2. Theorem (Skolem–Noether)**.** *For a central simple algebra D over a field F, the inclusion $D^{\times}/F^{\times} \hookrightarrow \mathrm{Aut}_F(D)$ carrying $u \in D^{\times}$ to $(d \mapsto udu^{-1})$ is an equality. That is, all automorphisms are inner.*

PROOF. This is [**53**, §4.6, Cor. to Thm. 4.9]. □

We finish our discussion of central simple algebras by using the Skolem–Noether theorem to build the K-linear *reduced trace* map $\mathrm{Trd}_{D/K} : D \to K$ for a central simple algebra D over a field K.

1.2.3.3. Construction. Let D be a central simple algebra over an arbitrary field K. It splits over a separable closure K_s, which is to say that there is a K_s-algebra isomorphism $f : D_{K_s} \simeq \mathrm{Mat}_n(K_s)$ onto the $n \times n$ matrix algebra for some $n \geqslant 1$. By the Skolem-Noether theorem, all automorphisms of a matrix algebra are given by conjugation by an invertible matrix. Hence, f is well-defined up to composition with an inner automorphism.

The matrix trace map $\mathrm{Tr} : \mathrm{Mat}_n(K_s) \to K_s$ is invariant under inner automorphisms and is equivariant for the natural action of $\mathrm{Gal}(K_s/K)$, so the composition of the matrix trace with f is a K_s-linear map $D_{K_s} \to K_s$ that is independent of f and $\mathrm{Gal}(K_s/K)$-equivariant. Thus, this descends to a K-linear map $\mathrm{Trd}_{D/K} : D \to K$ that is defined to be the *reduced trace.* In other words, the reduced trace map is a twisted form of the usual matrix trace, just as D is a twisted form of a matrix algebra. (For $d \in D$, the K-linear left multiplication map $x \mapsto d \cdot x$ on D has trace $\sqrt{[D:K]}\,\mathrm{Trd}_{D/K}(x)$, as we can see by scalar extension to K_s and a direct computation for matrix algebras. The elimination of the coefficient $\sqrt{[D:K]}$ is the reason for the word "reduced".)

1.2.4. Brauer groups. For applications to abelian varieties it is important to classify division algebras of finite dimension over $\mathbb{Q}$ (such as the endomorphism algebra of a simple abelian variety over a field). If Δ is such a ring then its center Z is a number field and Δ is a central division algebra over Z. More generally, the set of isomorphism classes of central division algebras over an arbitrary field has an interesting abelian group structure. This comes out of the following definition.

1.2.4.1. Definition. Central simple algebras D and D' over a field K are *similar* if there exist $n, n' \geqslant 1$ such that the central simple K-algebras $D \otimes_K \mathrm{Mat}_n(K) = \mathrm{Mat}_n(D)$ and $D' \otimes_K \mathrm{Mat}_{n'}(K) = \mathrm{Mat}_{n'}(D')$ are K-isomorphic.

The *Brauer group* $\mathrm{Br}(K)$ is the set of similarity classes of central simple algebras over K, and $[D]$ denotes the similarity class of D. For classes $[D]$ and $[D']$, define

$$[D][D'] := [D \otimes_K D'].$$

This composition law on $\mathrm{Br}(K)$ is well-defined and makes it into an abelian group with inversion given by $[D]^{-1} = [D^{\mathrm{opp}}]$, where D^{opp} is the "opposite algebra". By Proposition 1.2.2.2, each element in $\mathrm{Br}(K)$ is represented (up to isomorphism) by a unique central division algebra over K. In this sense, $\mathrm{Br}(K)$ is an abelian group structure on the set of isomorphism classes of such division algebras.

1.2.4.2. Example. The computation of the Brauer group of a number field involves computing the Brauer groups of local fields, so we now clear up any possible confusion concerning sign conventions in the description of Brauer groups for non-archimedean local fields. Upon choosing a separable closure K_s of an arbitrary field K, there are two natural procedures to define a functorial group isomorphism $\mathrm{Br}(K) \simeq \mathrm{H}^2(K_s/K, K_s^\times)$: a conceptual method via non-abelian cohomology as in [**107**, Ch. X, §5] and an explicit method via crossed-product algebras. By [**107**, Ch. X, §5, Exer. 2], these procedures are negatives of each other. We use the conceptual method of non-abelian cohomology, but we do not need to make that method explicit here and so we refer the interested reader to [**107**] for the details.

Let K be a non-archimedean local field with residue field κ and let K^{un} denote its maximal unramified subextension in K_s (with $\overline{\kappa}$ the residue field of K^{un}). It is known from local class field theory that the natural map $\mathrm{H}^2(K^{\mathrm{un}}/K, K^{\mathrm{un}\times}) \to \mathrm{H}^2(K_s/K, K_s^\times)$ is an isomorphism, and the normalized valuation mapping $K^{\mathrm{un}\times} \to \mathbb{Z}$ induces an isomorphism

$$\begin{aligned} \mathrm{H}^2(K^{\mathrm{un}}/K, K^{\mathrm{un}\times}) \simeq \mathrm{H}^2(K^{\mathrm{un}}/K, \mathbb{Z}) &\overset{\delta}{\simeq} \mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{un}}/K), \mathbb{Q}/\mathbb{Z}) \\ &= \mathrm{H}^1(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbb{Q}/\mathbb{Z}). \end{aligned}$$

There now arises the question of choice of topological generator for $\mathrm{Gal}(\overline{\kappa}/\kappa)$: arithmetic or geometric Frobenius? We choose to work with arithmetic Frobenius. (In [**103**, §1.1] and [**107**, Ch. XIII, §3] the arithmetic Frobenius generator is also used.)

Via evaluation on the chosen topological generator, our conventions lead to a composite isomorphism

$$\mathrm{inv}_K : \mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$$

for non-archimedean local fields K. If one uses the geometric Frobenius convention, then by also adopting the crossed-product algebra method to define the isomorphism

$$\mathrm{Br}(K) \simeq \mathrm{H}^2(K_s/K, K_s^\times)$$

one would get the *same* composite isomorphism inv_K since the two sign differences cancel out in the composite. (Beware that in [**103**] and [**107**] the Brauer group of a general field K is *defined* to be $\mathrm{H}^2(K_s/K, K_s^\times)$, and so the issue of choosing between non-abelian cohomology or crossed-product algebras does not arise in the foundational aspects of the theory. However, this issue implicitly arises in the relationship of Brauer groups and central simple algebras, such as in [**103**, Appendix to §1] where the details are omitted.)

Since $\mathrm{Br}(\mathbb{R})$ is cyclic of order 2 and $\mathrm{Br}(\mathbb{C})$ is trivial, for archimedean local fields K there is a unique injective homomorphism $\mathrm{inv}_K : \mathrm{Br}(K) \hookrightarrow \mathbb{Q}/\mathbb{Z}$.

By [**103**, §1.1, Thm. 3], for a finite extension K'/K of non-archimedean local fields, composition with the natural map $r^K_{K'} : \mathrm{Br}(K) \to \mathrm{Br}(K')$ satisfies

$$\mathrm{inv}_{K'} \circ r^K_{K'} = [K' : K] \cdot \mathrm{inv}_K. \tag{1.2.4.1}$$

By [**107**, Ch. XIII, §3, Cor. 3], $\mathrm{inv}_K(\Delta)$ has order $\sqrt{[\Delta : K]}$ for any central division algebra Δ over K. These assertions are trivially verified to hold for archimedean local fields K as well.

1.2.4.3. Theorem. *Let L be a global field. There is an exact sequence*

$$0 \longrightarrow \mathrm{Br}(L) \longrightarrow \bigoplus_v \mathrm{Br}(L_v) \xrightarrow{\sum \mathrm{inv}_{L_v}} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

where the direct sum is taken over all places of L and the first map is defined via extension of scalars.

Proof. This is [**120**, §9.7, §11.2]. □

For a global field L and central division algebra Δ over L, $\mathrm{inv}_v(\Delta)$ denotes $\mathrm{inv}_{L_v}(\Delta_{L_v})$. Theorem 1.2.4.3 says that a central division algebra Δ over a global field L is uniquely determined up to isomorphism by its invariants $\mathrm{inv}_v(\Delta)$, and that these may be arbitrarily assigned subject to the conditions $\mathrm{inv}_v(\Delta) = 0$ for all but finitely many v and $\sum \mathrm{inv}_v(\Delta) = 0$. Moreover, the order of $[\Delta]$ in $\mathrm{Br}(L)$ is the least common "denominator" of the local invariants $\mathrm{inv}_v(\Delta) \in \mathbb{Q}/\mathbb{Z}$.

If K is any field then for a class $c \in \mathrm{Br}(K)$ its *period* is its order and its *index* is $\sqrt{[\Delta : K]}$ with Δ the unique central division algebra over K representing the class c. It is a classical fact that the period divides that index and that these integers have the same prime factors (see [**107**, X.5], especially Lemma 1 and Exercise 3), but in general equality does not hold. For example, there are function fields of complex 3-folds for which some order-2 elements in the Brauer group cannot be represented by a quaternion algebra; examples are given in [**61**, §4], and there are examples with less interesting fields as first discovered by Brauer. We have noted above that over local fields there is equality of period and index (the archimedean case being trivial). The following deep result is an analogue over global fields.

1.2.4.4. Theorem. *For a central division algebra Δ over a global field L, the order of $[\Delta]$ in $\mathrm{Br}(L)$ is $\sqrt{[\Delta : L]}$.*

As a special (and very important) case, elements of order 2 in $\mathrm{Br}(L)$ are precisely the Brauer classes of quaternion division algebras for a global field L; as noted above, this fails for more general fields. Since Theorem 1.2.4.4 does not seem to be explicitly stated in any of the standard modern references on class field theory (though there is an allusion to it at the end of [**4**, Ch. X, §2]), and the structure theory of endomorphism algebras of abelian varieties rests on it, here is a proof.

Proof. Let Δ have degree n^2 over L and let d be the order of $[\Delta]$ in $\mathrm{Br}(L)$, so $d|n$. Note that d is the least common multiple of the local orders d_v of $[\Delta_{L_v}] \in \mathrm{Br}(L_v)$ for each place v of L, with $d_v = 1$ for complex v, $d_v|2$ for real v, and $d_v = 1$ for all but finitely many v. Using these formal properties of the d_v's, we may call upon the full power of global class field theory via Theorem 6 in [**4**, Ch. X] to infer the existence of a cyclic extension L'/L of degree d such that $[L'_{v'} : L_v]$ is a multiple of d_v for every place v of L (here, v' is any place on L' over v, and the constraint on the local degree is only non-trivial when $d_v > 1$). In the special case $d = 2$ (the only case we will require) one only needs weak approximation and Krasner's Lemma rather than class field theory: take L' to split a separable quadratic polynomial over L that closely approximates ones that define quadratic separable extensions of L_v for each v such that $d_v = 2$.

By (1.2.4.1), restriction maps on local Brauer groups induce multiplication by the local degree on the local invariants, so $\Delta_{L'}$ is locally split at all places of L'. Thus, by the injectivity of the map from the global Brauer group into the direct sum of the local ones (for L') we conclude that the Galois extension L'/L *of degree* d splits Δ. (The existence of cyclic splitting fields for all Brauer classes is proved for number fields in [**120**] and is proved for all global fields in [**128**], but neither reference seems to control the degree of the global cyclic extension.) It is a general fact for Brauer groups of arbitrary fields [**107**, Ch. X, §5, Lemma 1] that every Brauer class split by a Galois extension of degree r is represented by a central simple algebra with degree r^2. Applying this fact from algebra in our situation, $[\Delta] = [D]$ for a central simple algebra D of degree d^2 over L. But each Brauer class is represented by a unique central division algebra, and so D must be L-isomorphic to a matrix algebra over Δ. Since $[D : L] = d^2$ and $[\Delta : L] = n^2$ with $d|n$, this forces $d = n$ as desired. □

1.2.5. Homomorphisms and isotypicity. The study of maps between abelian varieties over a field rests on the following useful injectivity result.

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

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

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

Proof. Without loss of generality, K is algebraically closed (and hence perfect). When $\ell \neq \mathrm{char}(K)$ the assertion is a reformulation of the well-known analogous injectivity with ℓ-adic Tate modules (and such injectivity in turn underlies the proof of $\mathbb{Z}$-module finiteness of $\mathrm{Hom}(A, B)$). The proof in terms of Tate modules is given in [**82**, §19, Thm. 3] for $\ell \neq \mathrm{char}(K)$, and when phrased in terms of ℓ-divisible groups it works even when $\ell = p = \mathrm{char}(K) > 0$. For the convenience of the reader, we now provide the argument for $\ell = p$ in such terms. We will use that the torsion-free $\mathbb{Z}$-module $\mathrm{Hom}(A, B)$ is finitely generated, and our argument works for any ℓ (especially $\ell = \mathrm{char}(K)$).

Choose a $\mathbb{Z}$-basis $\{f_1, \dots, f_n\}$ of $\mathrm{Hom}(A, B)$. For $c_1, \dots, c_n \in \mathbb{Z}_\ell$ it suffices to show that if $\sum c_i f_i$ kills $A[\ell]$ then $\ell | c_i$ for all i. Indeed, if we can prove this then consider the case when $\sum c_i f_i$ kills $A[\ell^\infty]$. Certainly $c_i = \ell c_i'$ for some $c_i' \in \mathbb{Z}_\ell$, and $(\sum c_i' f_i) \cdot \ell$ kills $A[\ell^n]$ for all $n > 0$. But the map $A[\ell^n] \to A[\ell^{n-1}]$ induced by ℓ-multiplication is faithfully flat since it is the pullback along $A[\ell^{n-1}] \hookrightarrow A$ of the faithfully flat map $\ell : A \to A$, so $\sum c_i' f_i$ kills $A[\ell^{n-1}]$ for all $n > 0$. In other words, the kernel of the map in the Proposition would be ℓ-divisible, yet this kernel is a finitely generated $\mathbb{Z}_\ell$-module, so it would vanish as desired.

Now consider $c_1, \dots, c_n \in \mathbb{Z}_\ell$ such that $\sum c_i f_i$ kills $A[\ell]$. For the purpose of proving $c_i \in \ell\mathbb{Z}_\ell$ for all i, it is harmless to add to each c_i any element of $\ell\mathbb{Z}_\ell$. Hence, we may and do assume $c_i \in \mathbb{Z}$ for all i, so $\sum c_i f_i : A \to B$ makes sense and kills $A[\ell]$. Since $\ell : A \to A$ is a faithfully flat homomorphism with kernel $A[\ell]$, by fppf descent theory any K-group scheme homomorphism $A \to G$ that kills $A[\ell]$ factors through $\ell : A \to A$ (see [**30**, IV, 5.1.7.1] and [**98**]). Thus, $\sum c_i f_i = \ell \cdot h$ for some $h \in \mathrm{Hom}(A, B)$. Writing $h = \sum m_i f_i$ with $m_i \in \mathbb{Z}$, we get $\sum c_i \otimes f_i = \ell \cdot \sum 1 \otimes m_i f_i$ in $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(A, B)$. This implies $c_i = \ell m_i$ for all i, so we are done. □

A weakening of simplicity that is sometimes convenient is:

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

Clearly $\mathrm{End}^0(A)$ is a semisimple $\mathbb{Q}$-algebra. It is simple if and only if A is isotypic, and it is a division algebra if and only if A is simple.

By the Poincaré reducibility theorem, every non-zero abelian variety A over a field K is naturally isogenous to the product of its distinct isotypic parts, and these distinct parts admit no non-zero maps between them. Hence, if $\{B_i\}$ is the set of isotypic parts of A then $\mathrm{End}^0(A) = \prod \mathrm{End}^0(B_i)$ with each $\mathrm{End}^0(B_i)$ a simple algebra of finite dimension over $\mathbb{Q}$. Explicitly, if C_i is the unique simple factor of B_i then a choice of isogeny $B_i \to C_i^{e_i}$ defines an isomorphism from $\mathrm{End}^0(B_i)$ onto the matrix algebra $\mathrm{Mat}_{e_i}(\mathrm{End}^0(C_i))$ over the division algebra $\mathrm{End}^0(C_i)$. Beware that the composite "diagonal" ring map $\mathrm{End}^0(C_i) \to \mathrm{Mat}_{e_i}(\mathrm{End}^0(C_i)) \simeq \mathrm{End}^0(B_i)$ is canonical only when $\mathrm{End}^0(C_i)$ is commutative.

In general isotypicity is not preserved by extension of the ground field. To make examples illustrating this possibility, as well as other examples in the theory of abelian varieties, we need the operation of *Weil restriction of scalars*. For a field K and finite K-algebra K', the Weil restriction functor $\mathrm{Res}_{K'/K}$ from quasi-projective K'-schemes to separated (even quasi-projective) K-schemes of finite type is characterized by the functorial identity $\mathrm{Res}_{K'/K}(X')(A) = X'(K' \otimes_K A)$ for K-algebras A. Informally, Weil restriction is an algebraic analogue of viewing a complex manifold as a real manifold with twice the dimension. In particular, if K'/K is an extension of fields then $\mathrm{Res}_{K'/K}(X')$ is K'-smooth and equidimensional when X' is K-smooth and equidimensional, with

$$\dim(\mathrm{Res}_{K'/K}(X')) = [K' : K] \cdot \dim(X').$$

We refer the reader to [**10**, §7.6] for a self-contained development of the construction and properties of Weil restriction (replacing K with more general rings), and to [**25**, A.5] for a discussion of further properties (especially of interest for group schemes). In general the formation of Weil restriction naturally commutes with any extension of the base field, and for K' equal to the product ring K^n we have that $\mathrm{Res}_{K'/K}$ carries a disjoint union $\coprod_{i=1}^n S_i$ of quasi-projective K-schemes (viewed as a K'-scheme) to the product $\prod S_i$. Thus, the natural isomorphism

$$\mathrm{Res}_{K'/K}(X')_{K_s} \simeq \mathrm{Res}_{(K' \otimes_K K_s)/K_s}(X'_{K' \otimes_K K_s})$$

implies that if K' is a field separable over K then $\mathrm{Res}_{K'/K}(A')$ is an abelian variety over K of dimension $[K' : K]\dim(A')$ for any abelian variety A' over K' (since $K' \otimes_K K_s \simeq K_s^{[K':K]}$). If K'/K is a field extension of finite degree that is not separable then $\mathrm{Res}_{K'/K}(X')$ is never proper when X' is smooth and proper of positive dimension [**25**, Ex. A.5.6].

1.2.6. Example. Consider a separable quadratic extension of fields K'/K and a simple abelian variety A' over K'. Let $\sigma \in \mathrm{Gal}(K'/K)$ be the non-trivial element, so $K' \otimes_K K' \simeq K' \times K'$ via $x \otimes y \mapsto (xy, \sigma(x)y)$. Thus, the Weil restriction $A := \mathrm{Res}_{K'/K}(A')$ satisfies $A_{K'} \simeq A' \times \sigma^*(A')$, so $A_{K'}$ is not isotypic if and only if A' is not isogenous to its σ-twist. Hence, for $K = \mathbb{R}$ examples of non-isotypic

$A_{K'}$ are obtained by taking A' to be an elliptic curve over $\mathbb{C}$ with analytic model $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ for $\tau \in \mathbb{C} - \mathbb{R}$ such that $1, \tau, \overline{\tau}, \tau\overline{\tau}$ are $\mathbb{Q}$-linearly independent. (In Example 1.6.4 we give examples with $K = \mathbb{Q}$.)

In cases when $A_{K'}$ is non-isotypic, A is necessarily simple. Indeed, if A is not simple then a simple factor of A would be a K-descent of a member of the isogeny class of A', contradicting that A' and $\sigma^*(A')$ are not isogenous. Thus, we have exhibited examples in characteristic 0 for which isotypicity is lost after a ground field extension.

The failure of isotypicity to be preserved after a ground field extension does not occur over finite fields:

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

PROOF. By the Poincaré reducibility theorem, it is equivalent to show that $\mathrm{End}^0(A_{K'})$ is a simple $\mathbb{Q}$-algebra, so by Lemma 1.2.1.2 we may replace K' with the algebraic closure of K in K'. That is, we can assume that K'/K is algebraic. Writing $K' = \varinjlim K'_i$ with $\{K'_i\}$ denoting the directed system of subfields of finite degree over K, we have $\mathrm{End}(A_{K'}) = \varinjlim \mathrm{End}(A_{K'_i})$. But $\mathrm{End}(A_{K'})$ is finitely generated as a $\mathbb{Z}$-module, so for large enough i we have $\mathrm{End}^0(A_{K'}) = \mathrm{End}^0(A_{K'_i})$. We may therefore replace K' with K'_i for sufficiently large i to reduce to the case when K'/K is of finite degree. Let $q = \#K$.

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

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

1.3. Complex multiplication

1.3.1. Commutative subrings of endomorphism algebras. The following fact motivates the study of complex multiplication in the sense that we shall consider.

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

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

Since $D = \mathrm{End}^0(A)$ is of finite rank over $\mathbb{Q}$, clearly $[L : \mathbb{Q}]$ is finite. Choose a prime ℓ different from $\mathrm{char}(K)$. Recall that $V_\ell(A)$ denotes $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A)$ for $T_\ell(A) := \varprojlim A[\ell^n](K_s)$. The injectivity of the natural map

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

(see Proposition 1.2.5.1) implies that L_ℓ acts faithfully on the $\mathbb{Q}_\ell$-vector space $V_\ell(A)$ of rank $2g$. But $L_\ell = \prod_{w|\ell} L_w$, where w runs over all ℓ-adic places of L, so each corresponding factor module $V_\ell(A)_w$ over L_w is non-zero as a vector space over L_w. Hence,

$$2g = \dim_{\mathbb{Q}_\ell} V_\ell(A) = \sum_{w|\ell} \dim_{\mathbb{Q}_\ell} V_\ell(A)_w \geqslant \sum_{w|\ell} [L_w : \mathbb{Q}_\ell] = [L : \mathbb{Q}]$$

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

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

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

$$Z(P)_\ell = \mathbb{Q}_\ell \otimes_{\mathbb{Q}} Z(P) \to \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$$

is injective (Proposition 1.2.5.1) and lands inside $\mathrm{End}_{P_\ell}(V_\ell(A)) = P_\ell$. In other words, the inclusion $P \subset Z(P)$ of $\mathbb{Q}$-algebras becomes an equality after scalar extension to $\mathbb{Q}_\ell$, so $P = Z(P)$ as desired. □

The preceding theorem justifies the interest in the following concept.

1.3.1.2. Definition. An abelian variety A of dimension $g > 0$ over a field K admits *sufficiently many complex multiplications* (over K) if there exists a commutative semisimple $\mathbb{Q}$-subalgebra P in $\mathrm{End}^0(A)$ with rank $2g$ over $\mathbb{Q}$.

The reason for the terminology in Definition 1.3.1.2 is due to certain examples with $K = \mathbb{C}$ and P a number field such that the analytic uniformization of $A(\mathbb{C})$ expresses the P-action in terms of multiplication of complex numbers; see Example 1.5.3. The classical theory of complex multiplication focused on the case of Definition 1.3.1.2 in which P is a field, but it is useful to allow P to be a product of several fields (i.e., a commutative semisimple $\mathbb{Q}$-algebra). For example, by Theorem 1.3.1.1 this is necessary if we wish to consider the theory of complex multiplication with A that is not isotypic, or more generally if we want Definition 1.3.1.2 to be preserved under the formation of products. The theory of Shimura varieties provides further reasons not to require P to be a field.

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

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

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

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

See Definition 1.2.5.2 for the terminology used in (2).

PROOF. Let $\{B_i\}$ be the set of isotypic parts of A, so $\mathrm{End}^0(B_i) \simeq \mathrm{Mat}_{e_i}(\mathrm{End}^0(C_i))$ where C_i is the unique simple factor of B_i and $e_i \geqslant 1$ is its multiplicity as such. Since $\mathrm{End}^0(A) = \prod \mathrm{End}^0(B_i)$, (2) implies (1). It is clear that (3) implies (2).

Conversely, assume that $\mathrm{End}^0(A)$ contains a $\mathbb{Q}$-algebra P satisfying $[P : \mathbb{Q}] = 2\dim(A)$. There is a unique decomposition $P = \prod L_i$ with fields $L_1, \dots, L_s$, and $\sum [L_i : \mathbb{Q}] = 2\dim(A)$. We saw in the proof of Theorem 1.3.1.1 that by replacing A with an isogenous abelian variety we may arrange that $A = \prod A_i$ with each A_i a non-zero abelian variety having $L_i \subset \mathrm{End}^0(A_i)$ compatibly with the embedding $\prod \mathrm{End}^0(A_i) \subset \mathrm{End}^0(A)$ and the equality $\prod L_i = P$. Thus, $[L_i : \mathbb{Q}] \leqslant 2\dim(A_i)$ for all i (by Theorem 1.3.1.1), and adding this up over all i yields an equality, so each A_i admits sufficiently many complex multiplications using L_i. Since each simple factor of A is a simple factor of some A_i, to prove (3) we are therefore reduced to the case when $P = L$ is a field.

Applying Theorem 1.3.1.1 once again, L is its own centralizer in $\mathrm{End}^0(A)$ and A is isotypic, say with unique simple factor C appearing with multiplicity e. In particular, $\mathrm{End}^0(A) = \mathrm{Mat}_e(D)$ for the division algebra $D = \mathrm{End}^0(C)$ of finite rank over $\mathbb{Q}$. If Z denotes the center of D then D is a central division algebra over Z, and L contains Z since L is its own centralizer in $\mathrm{End}^0(A) = \mathrm{Mat}_e(D)$. Letting $d = \dim(C)$, $\mathrm{Mat}_e(D)$ contains the maximal commutative subfield L of degree $2g/[Z : \mathbb{Q}] = (2d/[Z : \mathbb{Q}])e$ over Z.

As we noted in the proof of Proposition 1.2.3.1 (parts of which are carried out for central simple algebras that may not be division algebras), the Z-degree of

$\mathrm{Mat}_e(D)$ is the product of the Z-degrees of L and the centralizer of L in $\mathrm{Mat}_e(D)$. But L is its own centralizer, so

$$e^2[D:Z] = \dim_Z \mathrm{Mat}_e(D) = [L:Z]^2 = e^2(2d/[Z:\mathbb{Q}])^2.$$

We conclude that $2d/[Z:\mathbb{Q}] = \sqrt{[D:Z]}$, so (by Proposition 1.2.3.1) $2d/[Z:\mathbb{Q}]$ is the common Z-degree of all maximal commutative subfields of the central division algebra $D = \mathrm{End}^0(C)$ over Z, or equivalently $2d$ is the $\mathbb{Q}$-degree of all such fields. But $2d = 2\dim(C)$, so choosing any maximal commutative subfield of D shows that C admits sufficiently many complex multiplications. □

1.3.3. CM algebras and CM abelian varieties. The following three conditions on a number field L are equivalent:

(1) L has no real embeddings but is quadratic over a totally real subfield,
(2) for every embedding $j : L \to \mathbb{C}$, the subfield $j(L) \subset \mathbb{C}$ is stable under complex conjugation and the involution $x \mapsto j^{-1}(\overline{j(x)})$ in $\mathrm{Aut}(L)$ is non-trivial and independent of j,
(3) there is a non-trivial involution $\tau \in \mathrm{Aut}(L)$ such that for every embedding $j : L \to \mathbb{C}$ we have $j(\tau(x)) = \overline{j(x)}$ for all $x \in L$.

The proof of the equivalence is easy. When these conditions hold, τ in (3) is unique and its fixed field is the maximal totally real subfield $L^+ \subset L$ (over which L is quadratic). The case $L^+ = \mathbb{Q}$ corresponds to the case when L is an imaginary quadratic field.

1.3.3.1. Definition. A CM *field* is a number field L satisfying the equivalent conditions (1), (2), and (3) above. A CM *algebra* is a product $L_1 \times \cdots \times L_s$ of finitely many CM fields (with $s \geqslant 1$).

The reason for this terminology is due to the following important result (along with Example 1.5.3).

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

The proof of this theorem (which ends with the proof of Lemma 1.3.7.1) will require some effort, especially since we consider an arbitrary base field K. Before we start the proof, it is instructive to consider an example.

1.3.4.1. Example. Consider $A = E^2$ with an elliptic curve E over $K = \mathbb{C}$ such that $L := \mathrm{End}^0(E)$ is an imaginary quadratic field. The endomorphism algebra $\mathrm{End}^0(A) = \mathrm{Mat}_2(L)$ is simple and contains as its maximal commutative subfields all quadratic extensions of L. Those extensions which are biquadratic over $\mathbb{Q}$ are CM fields, and the rest are not CM fields. Hence, in the setup of Theorem 1.3.4, even when A is isotypic and $\mathrm{char}(K) = 0$ there can be maximal commutative semisimple subalgebras of $\mathrm{End}^0(A)$ that are not CM algebras. However, if $\mathrm{char}(K) = 0$ and A is simple (over K) then $\mathrm{End}^0(A)$ is a CM field; see Proposition 1.3.6.4.

1.3.5. We will begin the proof of Theorem 1.3.4 now, but at a certain point we will need to use deeper input concerning the fine structure of endomorphism algebras of simple abelian varieties over general fields. At that point we will digress to review the required structure theory, and then we will complete the argument.

By Proposition 1.3.2.1, every simple factor of A admits sufficiently many complex multiplications. Thus, to prove the existence of the CM subalgebra P in Theorem 1.3.4 it suffices to treat the case when A is simple. Note that in the simple case such a CM subalgebra is automatically a field, since the endomorphism algebra is a division algebra. Let us first show that the result in the simple case implies that in the general isotypic case we can find P as a CM field. For isotypic A, by passing to an isogenous abelian variety we can arrange that $A = A'^m$ for a simple abelian variety A' over K and some $m \geqslant 1$. Thus, if $g' = \dim A'$ then $g = mg'$ and $\mathrm{End}^0(A')$ contains a CM field P' of degree $2g'$ over $\mathbb{Q}$. But $\mathrm{End}^0(A) \simeq \mathrm{Mat}_m(\mathrm{End}^0(A'))$ and this contains $\mathrm{Mat}_m(P')$. To find a CM field $P \subset \mathrm{End}^0(A)$ of degree $2g = 2g'm$ over $\mathbb{Q}$ it therefore suffices to construct a degree-m extension field P of P' such that P is a CM field.

Let P'^+ be the maximal totally real subfield of P', so for any totally real field P^+ of finite degree over P'^+ the ring $P = P^+ \otimes_{P'^+} P'$ is a field quadratic over P^+ and it is totally complex, so it is a CM field and clearly $[P : \mathbb{Q}] = [P : P'][P' : \mathbb{Q}] = 2g'[P^+ : P'^+]$. Hence, to find the required CM field P in the isotypic case it suffices to construct a degree-m totally real extension of P'^+. To do this, first recall the following basic fact from number theory [**15**, §6]:

1.3.5.1. Theorem (weak approximation)**.** *For any number field L and finite set S of places of L, the map $L \to \prod_{v \in S} L_v$ has dense image.*

Proof. This is [**15**, §6]. □

Applying this to P'^+, we can construct a monic polynomial f of degree m in $P'^+[u]$ that is very close to a totally split monic polynomial of degree m at each real place and is very close to an irreducible (e.g., Eisenstein) polynomial at a single non-archimedean place. It follows that f is totally split at each real place of P'^+ and is irreducible over P'^+, so the ring $P^+ = P'^+[u]/(f)$ is a totally real field of degree m over P'^+ as required.

1.3.5.2. We may and do assume for the remainder of the argument that A is simple. In this case $D = \mathrm{End}^0(A)$ is a central division algebra over a number field Z, so the commutative semisimple $\mathbb{Q}$-subalgebra $P \subset D$ is a field, and the proof of Proposition 1.3.2.1 shows that the common $\mathbb{Q}$-degree of all maximal commutative subfields of D is $2g$. Hence, our problem is to construct a maximal commutative subfield of D that is a CM field.

Let $\mathrm{Trd}_{D/\mathbb{Q}} = \mathrm{Tr}_{Z/\mathbb{Q}} \circ \mathrm{Trd}_{D/Z}$, where $\mathrm{Trd}_{D/Z}$ is the reduced trace. An abelian variety over any field admits a polarization, so choose a polarization of A over K. Let $x \mapsto x^*$ denote the associated Rosati involution on D (so $(xy)^* = y^*x^*$ and $x^{**} = x$).

1.3.5.3. Lemma. *The quadratic form $x \mapsto \mathrm{Trd}_{D/\mathbb{Q}}(xx^*)$ on D is positive-definite.*

Proof. For any central simple algebra D over any field K whatsoever, let $n = \sqrt{[D : K]}$ and define the variant $\mathrm{Trm}_{D/K} : D \to K$ of the reduced trace to be the map that sends each $y \in D$ to the trace of the K-linear map $m_y : D \to D$ defined by $d \mapsto yd$. We have $\mathrm{Trm}_{D/K} = n \cdot \mathrm{Trd}_{D/K}$, as may be checked by extending scalars to K_s and directly computing with elementary matrices (see 1.2.3.3). Hence, in the setting of interest with $D = \mathrm{End}^0(A)$ and $K = Z$ we see that it is equivalent to prove positive-definiteness for the quadratic form $x \mapsto \mathrm{Trm}_{D/\mathbb{Q}}(xx^*)$, where $\mathrm{Trm}_{D/\mathbb{Q}} = \mathrm{Tr}_{Z/\mathbb{Q}} \circ \mathrm{Trm}_{D/Z}$. The positive-definiteness for $\mathrm{Trm}_{D/\mathbb{Q}}$ can be verified by replacing D with $\mathrm{End}^0_{\overline{K}}(A_{\overline{K}})$, to which [**82**, §21, Thm. 1] applies. □

Lemma 1.3.5.3 says that $x \mapsto x^*$ is a *positive involution* of D (relative to the linear form $\mathrm{Trd}_{D/\mathbb{Q}}$). The existence of such an involution severely constrains the possibilities for D. First we record the consequences for the center Z.

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

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

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

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

1.3.6. Albert's classification. To go further with the proof of Theorem 1.3.4, we need to review properties of endomorphism algebras of simple abelian varieties over arbitrary fields.

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

For any Albert algebra D and any algebraically closed field K, there exists a simple abelian variety A over K such that $\mathrm{End}^0(A)$ is $\mathbb{Q}$-isomorphic to D (with the given involution on D arising from a polarization on A); see [**1**], [**2**], [**3**], [**112**, §4.1, Thm. 5], and [**46**, Thm. 13]. For a survey and further references on this topic, see [**92**]. We will not need this result.

Instead, we are interested in the non-trivial constraints on the Albert algebras that arise from polarized simple abelian varieties A over an arbitrary field K when $\mathrm{char}(K)$ and $\dim A$ are fixed. Before listing these constraints, it is convenient to record Albert's classification of general Albert algebras (omitting a description of the possibilities for the involution).

1.3.6.2. Theorem (Albert)**.** *Let $(D, (\cdot)^*)$ be an Albert algebra. For any place v of the center Z, let v^* denote the pullback of v along $x \mapsto x^*$. Exactly one of the following occurs:*

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

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

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

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

Proof. See [**82**, §21, Thm. 2] (which also records the possibilities for the involution). □

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

- whenever $\mathrm{char}(K) = 0$, the integer $ed^2 = [D : \mathbb{Q}]$ divides $2g$ (proof: there is a subfield $K_0 \subseteq K$ finitely generated over $\mathbb{Q}$ such that A descends to an abelian variety A_0 over K_0 and the D-action on A in the isogeny category over K descends to an action on A_0 in the isogeny category over K_0, so upon choosing an embedding $K_0 \hookrightarrow \mathbb{C}$ we get a $\mathbb{Q}$-linear action by the division algebra D on the $2g$-dimensional homology $\mathrm{H}_1(A_0(\mathbb{C}), \mathbb{Q})$),
- the action of D on $V_\ell(A)$ with $\ell \neq \mathrm{char}(K)$ implies (via Cor. to Thm. 4 of [**82**, §19], whose proof is valid over any base field) that $ed | 2g$,
- the structure of symmetric elements in

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(A, A^t) \simeq \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$$

  (via [**82**, §20, Cor. to Thm. 3], whose proof is valid over any base field) yields that $[L : \mathbb{Q}] | g$ for every commutative subfield $L \subset D$ whose elements are invariant under the involution.
- for Type II in any characteristic we have $2e | g$ (which coincides with the general divisibility $ed^2 | 2g$ when $\mathrm{char}(K) = 0$ since $d = 2$ for Type II). To prove it uniformly across all characteristics, first note that for Type II we have

$$\mathbb{R} \otimes_{\mathbb{Q}} D = (\mathbb{R} \otimes_{\mathbb{Q}} Z) \otimes_Z D = \prod_{v | \infty} Z_v \otimes_Z D \simeq \mathrm{Mat}_2(Z_v)^e.$$

Moreover, by [**82**, §21, Thm. 2] it can be arranged that under this composite isomorphism the positive involution on D goes over to transpose on each factor $\mathrm{Mat}_2(Z_v) = \mathrm{Mat}_2(\mathbb{R})$. Thus, for D of Type II the fixed part of the involution on D has $\mathbb{Q}$-dimension $2e$ and hence Z-degree 2. By centrality of Z in the division algebra D, the condition $x^* = x$ for x in D of Type II therefore defines a necessarily commutative quadratic extension Z' of Z inside D, so g is divisible by $[Z' : \mathbb{Q}] = 2e$ as desired.

The preceding results are summarized in the following table, taken from the end of [**82**, §21]. (As we have just seen, the hypothesis there that K is algebraically closed is not necessary.) The invariants of $D = \mathrm{End}^0(A)$ are given in the first three columns. In the last two columns we give some necessary divisibility restrictions on these invariants.

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

We refer the reader to [**82**, §21], and to [**92**] for further information on these invariants. Using the above table, we can prove the following additional facts when the simple A admits sufficiently many complex multiplications.

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

(1) *If* $\mathrm{char}(K) = 0$ *then D is of Type* IV *with $d = 1$ and $e = 2g$ (so D is a* CM *field, by Theorem* 1.3.6.2*).*
(2) *If* $\mathrm{char}(K) > 0$ *then D is of Type* III *or Type* IV*.*

Proof. By simplicity, D is a division algebra. Its center Z is a commutative field.

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

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

1.3.7. Returning to the proof of Theorem 1.3.4, recall that we reduced the proof to the case of simple A. Proposition 1.3.6.4(1) settles the case of characteristic 0, and Proposition 1.3.6.4(2) gives that $D = \mathrm{End}^0(A)$ is an Albert algebra of Type III or IV when $\mathrm{char}(K) > 0$. If D is of Type III then the center Z is totally real and d is even, whereas if D is of Type IV then Z is CM. Thus, we can apply the following general lemma to conclude the proof.

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

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

Proof. By Proposition 1.2.3.1, any degree-d extension of Z that splits D is a maximal commutative subfield of D. Hence, we just need to find a degree-d extension L of Z that is a CM field and splits D. Let Σ be a finite non-empty set of finite places of Z containing the finite places at which D is non-split. By the structure of Brauer groups of local fields, for any $v \in \Sigma$ the central simple Z_v-algebra

$$D_v := Z_v \otimes_Z D$$

of rank d^2 over Z_v is split by any extension of Z_v of degree d.

First assume that Z is totally real, so d is even. By weak approximation (Theorem 1.3.5.1), there is a monic polynomial f over Z of degree $d/2$ that is close to a monic irreducible polynomial of degree $d/2$ over Z_v for all $v \in \Sigma$ (and in particular f is irreducible over all such Z_v, and hence over Z since Σ is non-empty). We can also arrange that for each real place v of Z the polynomial f viewed over $Z_v \simeq \mathbb{R}$ is close to a totally split monic polynomial of degree $d/2$ and hence is totally split over Z_v. Thus, $Z' := Z[u]/(f)$ is a totally real extension field of Z with degree $d/2$. By the same method, we can construct a quadratic extension L/Z' that is unramified quadratic over each place v' over a place in Σ and is also totally complex (by using approximations to irreducible quadratics over $\mathbb{R}$ at the real places of Z'). This L is a CM field and it is designed so that $Z_v \otimes_Z L$ is a degree-d field extension of Z_v for all $v \in \Sigma$. Hence, D_L is split at all places of L (the archimedean ones being obvious), so D_L is split.

Assume next that Z is a CM field. Let $Z^+ \subset Z$ be the maximal totally real subfield. By the same weak approximation procedure as above (replacing $d/2$ with d), we can construct a degree d totally real extension ${Z'}^+/Z^+$ such that for each place v_0 of Z^+ beneath a place $v \in \Sigma$, the extension ${Z'}^+/Z^+$ has a unique place v_0' over v_0 and is totally ramified (resp. unramified) at v_0' when Z/Z^+ is unramified (resp. ramified) at v. Hence, $({Z'}^+)_{v_0'}$ and Z_v are linearly disjoint over $(Z^+)_{v_0}$. We conclude that ${Z'}^+$ and Z are linearly disjoint over Z', so $L := {Z'}^+ \otimes_{Z^+} Z$ is a field and each $v \in \Sigma$ has a unique place w over it in L. Clearly $[L_w : Z_v] = d$ for all such w, so L splits D. By construction, L is visibly CM. We have proved Lemma 1.3.7.1. This also finishes the proof of Theorem 1.3.4. □

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

PROOF. By Theorem 1.3.4, the endomorphism algebra $\mathrm{End}^0(A)$ contains a commutative field with $\mathbb{Q}$-degree $2\dim(A)$. This property is preserved after any ground field extension (even though the endomorphism algebra may get larger), so by the final part of Theorem 1.3.1.1 isotypicity is preserved as well. ☐

1.3.8. CM abelian varieties. It turns out to be convenient to view the CM algebra P in Theorem 1.3.4 as an abstract ring in its own right, and to thereby regard the embedding $P \hookrightarrow \mathrm{End}^0(A)$ as additional structure on A. This is encoded in the following concept.

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

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

As an application of Theorem 1.3.4, we establish the following result concerning the possibilities for Z of Type III in Proposition 1.3.6.4(2). This will not be used later.

1.3.8.2. Proposition. *Let A, K, and D be as in Proposition* 1.3.6.4(2) *with* $p = \mathrm{char}(K) > 0$*, and let Z be the center of D,* $g = \dim(A)$*,* $d = \sqrt{[D : Z]}$*, and* $e = [Z : \mathbb{Q}]$*. We have $ed = 2g$, and if D is of Type* III *(so* $d = 2$*) then either* $Z = \mathbb{Q}$ *or* $Z = \mathbb{Q}(\sqrt{p})$*.*

Note that in this proposition, K is an arbitrary field with $\mathrm{char}(K) > 0$; K is not assumed to be finite.

PROOF. We always have $ed|2g$, but $ed = \sqrt{[D : \mathbb{Q}]}$ and D contains a field P of $\mathbb{Q}$-degree $2g$, so $2g|ed$. Thus, $ed = 2g$. Now we can assume A is of Type III, so the field Z is totally real.

Since A is of finite type over K and D is finite-dimensional over $\mathbb{Q}$, by direct limit considerations we can descend to the case when K is finitely generated over $\mathbb{F}_p$. Let S be a separated integral $\mathbb{F}_p$-scheme of finite type whose function field is K. Since A is an abelian variety over the direct limit K of the coordinate rings of the non-empty affine open subschemes of S, by replacing S with a sufficiently small non-empty affine open subscheme we can arrange that A is the generic fiber of an abelian scheme $\mathscr{A} \to S$. Since S is connected, the fibers of the map $\mathscr{A} \to S$ all have the same dimension, and this common dimension is g (as we may compute using the generic fiber A).

The $\mathbb{Z}$-module $\mathrm{End}(A)$ is finitely generated, and each endomorphism of A extends uniquely to a U-endomorphism of $\mathscr{A}_U$ for some non-empty open U in S (with U perhaps depending on the chosen endomorphism). Using a finite set of endomorphisms that spans $\mathrm{End}(A)$ allows us to shrink S so that all elements of $\mathrm{End}(A)$ extend to S-endomorphisms of $\mathscr{A}$, or in other words $\mathrm{End}(A) = \mathrm{End}(\mathscr{A})$. We therefore have a specialization map $D = \mathrm{End}^0(A) \to \mathrm{End}^0(\mathscr{A}_s)$ for every $s \in S$.

Fix a prime $\ell \neq p$. Since S is connected and $\mathscr{A}[\ell^n]$ is finite étale over S, an S-endomorphism of $\mathscr{A}[\ell^n]$ is uniquely determined by its effect on a single geometric fiber over S. But maps between abelian varieties are uniquely determined by their effect on ℓ-adic Tate modules when ℓ is a unit in the base field, so we conclude (via consideration of ℓ-power torsion) that the specialization map $D \to \mathrm{End}^0(\mathscr{A}_s)$ is injective for all $s \in S$. We can therefore speak of an element of $\mathrm{End}^0(\mathscr{A}_s)$ "lifting" over K in the sense that it is the image of a unique element of $D = \mathrm{End}^0(A)$ under the specialization mapping at s. This will be of interest when s is a closed point and we consider the q_s-Frobenius endomorphism of $\mathscr{A}_s$ over the finite residue field $\kappa(s)$ at s (with $q_s = \#\kappa(s)$).

By Theorem 1.3.4, we can choose a CM field $L \subset D$ with $[L : \mathbb{Q}] = 2g$. In particular, for each $s \in S$ the field L embeds into $\mathrm{End}^0(\mathscr{A}_s)$ with $[L : \mathbb{Q}] = 2g = 2\dim(\mathscr{A}_s)$, so each $\mathscr{A}_s$ is isotypic. By Theorem 1.3.1.1, L is its own centralizer in $\mathrm{End}^0(\mathscr{A}_s)$. Take s to be a closed point of S, and let q_s denote the size of the finite residue field $\kappa(s)$ at s. The q_s-Frobenius endomorphism $\varphi_s \in \mathrm{End}^0(\mathscr{A}_s)$ is central, so it centralizes L and hence must lie in the image of L. In particular, φ_s lifts to an element of $\mathrm{End}^0(A) = D$ that is necessarily central (as we may compute after applying the injective specialization map $D \hookrightarrow \mathrm{End}^0(\mathscr{A}_s)$). That is, $\varphi_s \in Z \subset D$ for all closed points $s \in S$.

Let Z' be the subfield of Z generated over $\mathbb{Q}$ by the lifts of the endomorphisms φ_s as s varies through all closed points of S. Each $\mathbb{Q}[\varphi_s]$ is a totally real field since Z is totally real. By Weil's Riemann Hypothesis for abelian varieties over finite fields (see the discussion following Definition 1.6.1.2), under any embedding $\iota : \mathbb{Q}[\varphi_s] \hookrightarrow \mathbb{C}$ we have each $\iota(\varphi_s)\overline{\iota(\varphi_s)} = q_s$ for $q_s = \#\kappa(s) \in p^{\mathbb{Z}}$, so the real number $\iota(\varphi_s)$ is a power of $\sqrt{p}$. Hence, the subfield $\mathbb{Q}[\varphi_s] \subset Z$ is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$, so the subfield $Z' \subset Z$ is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$.

Let η be a geometric generic point of S, and let Γ be the associated absolute Galois group for the function field of S. Because each $\mathscr{A}[\ell^n]$ is finite étale over S, the representation of Γ on $V_\ell(A)$ factors through the quotient $\pi_1(S, \eta)$. The Chebotarev Density Theorem for $\pi_1(S, \eta)$ [**97**, App. B.9] says that the Frobenius elements at the closed points of S generate a dense subgroup of the quotient $\pi_1(S, \eta)$ of Γ. Thus, the image of $\mathbb{Q}_\ell[\Gamma]$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ is equal to the subalgebra $Z'_\ell := \mathbb{Q}_\ell \otimes_{\mathbb{Q}} Z'$ generated by the endomorphisms φ_s. We therefore have an injective map

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} D \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell[\Gamma]}(V_\ell(A)) = \mathrm{End}_{Z'_\ell}(V_\ell(A)).$$

By Zarhin's theorem [**134**] (see [**80**, XII, §2] for a proof valid for all p, especially allowing $p = 2$) this injection is an isomorphism, so we conclude that Z_ℓ is central in $\mathrm{End}_{Z'_\ell}(V_\ell(A))$. But the center of this latter matrix algebra is Z'_ℓ, so the inclusion $Z'_\ell \subset Z_\ell$ is an equality. Hence, the inclusion $Z' \subset Z$ is an equality as well. Since Z' is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$, we are done. □

1.4. Dieudonné theory, p-divisible groups, and deformations

To solve problems involving lifts from characteristic p to characteristic 0, we need a technique for handling p-torsion phenomena in characteristic $p > 0$. The two main tools for this purpose in what we shall do are Dieudonné theory and p-divisible groups. For the convenience of the reader we review the basic facts in this direction, and for additional details we refer to [**119**], [**110**, §6], and [**75**] for

p-divisible groups, and [**41**, Ch. II–III] for (contravariant) Dieudonné theory with applications to p-divisible groups.

1.4.1. Exactness. We shall frequently use exact sequence arguments with abelian varieties and finite group schemes over fields, as well as with their relative analogues over more general base schemes. It is assumed that the reader has some familiarity with these notions, but we now provide a review of this material.

1.4.1.1. Definition. Let S be a scheme, and let $\mathscr{T}$ be a Grothendieck topology on the category of S-schemes. (For our purposes, only the étale, fppf, and fpqc topologies will arise.) A diagram $1 \to G' \to G \xrightarrow{f} G'' \to 1$ of S-group schemes is *short exact* for the topology $\mathscr{T}$ if $G' \to G$ is an isomorphism onto $\ker(f)$ and the map f is a $\mathscr{T}$-covering.

By [**30**, Exp. IV, 5.1.7.1], in such cases G'' represents the quotient sheaf G/G' for the chosen Grothendieck topology. By [**31**, Exp. V, Thm. 4.1(iv), Rem. 5.1], if G is a quasi-projective group scheme over a noetherian ring R and if G' is a finite flat R-subgroup of G then the fppf quotient sheaf G/G' is represented by a quasi-projective R-group (also denoted G/G'), and the resulting map of group schemes $G \to G/G'$ is an fppf G'-torsor (so G/G' is R-flat if G is).

1.4.1.2. The *Cartier dual* N^D of a commutative finite locally free group scheme N over a base scheme S is the commutative finite locally free group scheme which represents the fppf sheaf functor $\mathscr{H}om(N, \mathbb{G}_{\mathrm{m}}) : S' \rightsquigarrow \mathrm{Hom}_{S'\text{-gp}}(N_{S'}, \mathbb{G}_{\mathrm{m}})$ on the category of S-schemes. The structure sheaf $\mathcal{O}_{N^D}$ of N^D is canonically isomorphic to the $\mathcal{O}_S$-linear dual of the structure sheaf $\mathcal{O}_N$ of N, and the co-multiplication (respectively multiplication) map for $\mathcal{O}_{N^D}$ is the $\mathcal{O}_S$-linear dual of the multiplication (respectively co-multiplication) map for $\mathcal{O}_N$.

The functor $N \rightsquigarrow N^D$ on the category of commutative finite locally free group schemes over S swaps closed immersions and quotient maps, preserves exactness, and is an involution in the sense that there is a natural isomorphism $f_N : N \simeq (N^D)^D$ satisfying $(f_N)^D = f_{N^D}^{-1}$. See [**87**, Prop. 2.9] for further details.

As an application, if the S-homomorphism $j : G' \hookrightarrow G$ is a closed immersion between finite locally free commutative group schemes then we can use Cartier duality to give a direct proof that the the fppf quotient sheaf G/G' is represented by a finite locally free S-group (without needing to appeal to general existence results for quotients by G'-actions on quasi-projective S-schemes). The key point is that the Cartier dual map $j^D : G^D \to G'^D$ between finite flat S-schemes is faithfully flat, as this holds on fibers over S (since injective maps between Hopf algebras over a field are always faithfully flat [**126**, 14.1]). Such flatness implies that $H := \ker(j^D)$ is a finite locally free commutative S-group, so H^D makes sense and the dual map $q : G \simeq (G^D)^D \to H^D$ is faithfully flat. It is clear that $G' \subset \ker(q)$, and this inclusion between finite locally free S-schemes is an isomorphism by comparison of fibral degrees, so H^D represents G/G'.

The following result is useful for constructing commutative group schemes $G \to S$ that are finite and fppf (equivalently, finite and locally free over S).

1.4.1.3. Proposition. *Let S be a scheme, and let G' and G'' be finitely presented separated S-group schemes with G' affine and flat over S. For any exact sequence*

$$1 \to G' \to G \to G'' \to 1$$

of group sheaves for the fppf topology on the category of S-schemes, G is represented by a finitely presented S-group that is flat and affine over G''. Moreover, G' and G'' are S-finite if and only if G is S-finite.

See [**87**, 17.4] for a generalization (using the fpqc topology).

Proof. For any G''-scheme T viewed as an S-scheme, let $g'' \in G''(T)$ correspond to the given S-morphism $T \to G''$. Consider the set $E_{g''}(T)$ that is the preimage under $G(T) \to G''(T)$ of g''. This is a sheaf of sets on the category of G''-schemes equipped with the fppf topology, and as such it is a left G'-torsor (strictly speaking, a left torsor for the G''-group $G'_{G''}$) due to the given exact sequence. In particular, the fppf sheaves of sets $E_{g''}$ and $G'_{G''}$ over G'' are isomorphic fppf-locally over G''.

Since G' is fppf affine over S and fppf descent is effective for affine morphisms, it follows that $E_{g''}$ as an fppf sheaf of sets over G'' is represented by an affine fppf G''-scheme (which is therefore affine fppf over S when G'' is). It is elementary to check that this affine G''-scheme viewed as an S-scheme has its functor of points naturally identified with G (since for any S-scheme T and $g \in G(T)$, visibly $g \in E_{g''}(T)$ for the point $g'' \in G''(T)$ arising from g), so G is represented by an S-group.

Separatedness of G'' over S and exactness imply that G' is closed in G. Moreover, $G \to G''$ is a left $G'_{G''}$-torsor for the fppf topology over G'', so it is finite when G' is S-finite. Thus, if G' and G'' are S-finite then G is S-finite. Conversely, if G is S-finite then its closed subscheme G' is S-finite, so the quotient G/G' exists as an S-finite scheme. But G'' represents this quotient, so G'' is S-finite too. □

1.4.1.4. Remark. If $1 \to G' \to G \to G'' \to 1$ is an exact sequence of separated fppf S-groups with G' and G'' abelian schemes then G is an abelian scheme. Indeed, since $G \to G''$ is an fppf torsor for the G''-group $G'_{G''}$ that is smooth and proper with geometrically connected fibers, $G \to G''$ is smooth and proper with geometrically connected fibers. The map $G'' \to S$ is also smooth and proper with geometrically connected fibers, so $G \to S$ is as well. Hence, G is an abelian scheme.

It is also true that if G is an abelian scheme and G' is a closed S-subgroup of G that is also an abelian scheme then the fppf quotient sheaf G/G' is represented by an abelian scheme. We will give an elementary proof of this over fields in Lemma 1.7.4.4 using the Poincaré reducibility theorem (which is only available over fields). In general the proof requires a detour through algebraic spaces.

1.4.2. Duality for abelian schemes. In [**83**, §6.1], duality is developed for projective abelian schemes, building on the case of an algebraically closed ground field. Projectivity is imposed primarily due to the projectivity hypotheses in Grothendieck's work on Hilbert schemes. The projective case is sufficient for our needs because any abelian scheme over a discrete valuation ring is projective (this follows from Lemma 2.1.1.1, to which the interested reader may now turn). For both technical and aesthetic reasons, it is convenient to avoid the projectivity hypothesis. We now sketch Grothendieck's results on duality in the projective case, as well as Artin's improvements that eliminated the projectivity assumption.

1.4.2.1. Let $A \to S$ be an abelian scheme, and let $\mathrm{Pic}_{A/S}$ be the functor assigning to any S-scheme T the group of isomorphism classes of pairs $(\mathscr{L}, i)$ consisting of an invertible sheaf $\mathscr{L}$ on A_T and a trivialization $i : e_T^*(\mathscr{L}) \simeq \mathcal{O}_T$ along the identity section e_T of $A_T \to T$. This is an fppf group sheaf on the category of S-schemes, and its restriction to the category of S'-schemes (for an S-scheme S') is $\mathrm{Pic}_{A_{S'}/S'}$.

Let $\mathrm{Pic}^0_{A/S} \subset \mathrm{Pic}_{A/S}$ be the subfunctor classifying pairs $(\mathscr{L}, i)$ that lie in the identity component of the Picard scheme on geometric fibers. By [**7**, Exp. XIII, Thm. 4.7(i)] (see [**39**, §9.6] for the projective case), the inclusion $j : \mathrm{Pic}^0_{A/S} \to \mathrm{Pic}_{A/S}$ is an open subfunctor; i.e., it is relatively representable by open immersions. This means that for any S-scheme T and $(\mathscr{L}, i) \in \mathrm{Pic}_{A/S}(T)$, $\mathrm{Pic}^0_{A/S} \times_{\mathrm{Pic}_{A/S}} T$ as a functor on T-schemes is represented by an open subscheme $U \subset T$; explicitly, there is an open subscheme $U \subset T$ such that a T-scheme T' lies over U if and only if the T'-pullback of $(\mathscr{L}, i)$ lies in Pic^0 on geometric fibers over T'.

By Grothendieck's work on Picard schemes (see [**39**, Part 5]), if $A \to S$ is projective Zariski-locally on S then $\mathrm{Pic}_{A/S}$ is represented by a locally finitely presented and separated S-scheme and the open subscheme A^t representing $\mathrm{Pic}^0_{A/S}$ is quasi-projective Zariski-locally on S and finitely presented. For noetherian S, functorial criteria show that A^t is proper and smooth (see [**83**, §6.1]), hence an abelian scheme; the case of general S (with A projective Zariski-locally on S) then follows by descent to the noetherian case.

To drop the projectivity hypothesis, one has to use algebraic spaces. Informally, an algebraic space over S is an fppf sheaf on the category of S-schemes that is "well-approximated" by a representable functor (relative to the étale topology), so concepts from algebraic geometry such as smoothness, properness, and connectedness can be defined and behave as expected; see [**60**]. By Artin's work on relative Picard functors as algebraic spaces (see [**5**, Thm. 7.3]), $\mathrm{Pic}_{A/S}$ is always a separated algebraic space locally of finite presentation, and by [**7**, Exp. XIII, Thm. 4.7(iii)] the open algebraic subspace $\mathrm{Pic}^0_{A/S}$ is finitely presented over S.

The functorial arguments that prove smoothness and properness for $\mathrm{Pic}^0_{A/S}$ when A is projective work without projectivity because the same criteria are available for algebraic spaces. Thus, $\mathrm{Pic}^0_{A/S}$ is smooth and proper over S in the sense of algebraic spaces. Consequently, by a theorem of Raynaud (see [**38**, Thm. 1.9]), $\mathrm{Pic}^0_{A/S}$ is represented by an S-scheme A^t; this must be an abelian scheme, called the *dual abelian scheme*. Its formation commutes with any base change on S, and it is contravariant in A in an evident manner.

1.4.2.2. Over $A \times A^t$ there is a Poincaré bundle $\mathscr{P}_{A/S}$ provided by the universal property of A^t, exactly as in the theory of duality for abelian varieties over a field. In particular, $\mathscr{P}_{A/S}$ is canonically trivialized along $e \times \mathrm{id}_{A^t}$. Let $e' \in A^t(S)$ be the identity, so for any S-scheme T the point $e'_T \in A^t(T)$ corresponds to $\mathcal{O}_{A_T}$ equipped with the canonical trivialization of $e_T^*(\mathcal{O}_{A_T})$. Thus, setting $T = A$ gives that $\mathscr{P}_{A/S}$ is also canonically trivialized along $\mathrm{id}_A \times e'$. Hence, the pullback of $\mathscr{P}_{A/S}$ along the flip $A^t \times A \simeq A \times A^t$ defines a canonical S-morphism $\iota_{A/S} : A \to A^{tt}$. This morphism carries the identity to the identity, so it is a homomorphism. By applying the duality theory over fields to the fibers of A over S, it follows that $\iota_{A/S}$ is an isomorphism; in other words, the pullback of $\mathscr{P}_{A/S}$ along the flip $A^t \times A \simeq A \times A^t$ is uniquely isomorphic to $\mathscr{P}_{A^t/S}$ respecting trivializations along the identity sections of both factors. Such uniqueness implies that $\iota^t_{A/S}$ is inverse to $\iota_{A^t/S}$.

A homomorphism $f : A \to A^t$ is *symmetric* when the map

$$f^t \circ \iota_{A/S} : A \simeq A^{tt} \to A^t$$

is equal to f. Writing $f^\dagger := f^t \circ \iota_{A/S}$, the equality $\iota^t_{A/S} = \iota^{-1}_{A^t/S}$ and the functoriality of $\iota_{A/S}$ in A (applied with respect to f) implies $f^{\dagger\dagger} = f$, so if we abuse notation by writing f^t rather than $f^\dagger$ then $(f^t)^t = f$. We say f is *symmetric* when $f^t = f$ (or more accurately, $f^\dagger = f$). This property holds if it does so on fibers over S, because homomorphisms $f, f' : A \rightrightarrows B$ between abelian schemes coincide if $f_s = f'_s$ for all $s \in S$. Indeed, for noetherian S such rigidity is [**83**, Cor. 6.2], and the general case reduces to this because equality on all fibers descends through direct limits (since it says that the finitely presented ideal of $(f, f')^{-1}(\Delta_{A/S})$ in $\mathcal{O}_A$ is nilpotent).

A *polarization* of A is a homomorphism $f : A \to A^t$ that is a polarization on geometric fibers. Any such f is necessarily symmetric. The properties of polarizations are developed in [**83**, §6.2] for projective abelian schemes, but the only purpose of imposing projectivity at the outset (even though it is a consequence of the definition, due to [**34**, IV$_3$, 9.6.4]) is to ensure the existence of the dual abelian scheme, so such an assumption may be eliminated.

1.4.2.3. Definition. A homomorphism $\varphi : A \to B$ between abelian schemes over a scheme S is an *isogeny* when it is surjective with finite fibers. (Equivalently, the homomorphims φ_s are isogenies in the sense of abelian varieties for each $s \in S$.)

Since quasi-finite proper morphisms are finite by [**34**, IV$_4$, 18.12.4] (or by [**34**, IV$_3$, 8.11.1] with finite presentation hypothesis, which suffices for us), any isogeny between abelian schemes is a finite morphism. Moreover, by the fibral flatness criterion [**34**, IV$_3$, 11.3.11], such maps are flat. Hence, if φ as above is an isogeny then it is finite locally free (and surjective), so the closed subgroup $\ker(\varphi)$ is a finite locally free commutative S-group scheme. Thus, B represents the fppf quotient sheaf $A/\ker(\varphi)$. For example, setting $\varphi = [n]_A$ for $n \geqslant 1$ gives $A/A[n] \simeq A$.

Turning this around, suppose we are given the abelian scheme A and a closed S-subgroup $N \subset A$ that is finite locally free over S. Consider the fppf quotient sheaf A/N. We claim that this quotient is (represented by) an abelian scheme, so the map $A \to A/N$ with kernel N is an isogeny. It suffices to work Zariski-locally on S, so we may assume that $N \to S$ has all fibers with the same order $n \geqslant 1$. We then have $N \subset A[n]$, due to the following result (proved in [**123**, §1]):

1.4.2.4. Theorem (Deligne). *Let S be a scheme and let H be a commutative S-group scheme for which the structural morphism $H \to S$ is finite and locally free. If the fibers H_s have rank n for all $s \in S$ then H is killed by n.*

The quotient sheaf A/N is an fppf torsor over $A/A[n] \simeq A$ with fppf covering group $A[n]/N$ that is finite (and hence *affine*) over S. It then follows from effective fppf descent for affine morphisms that the quotient A/N is represented by a scheme finite over $A/A[n] = A$, and the map $A \to A/N$ is an fppf $A[n]/N$-torsor, so the S-proper S-smooth A is finite locally free over A/N (as $A[n]/N$ is finite locally free over S). Hence, A/N is proper and smooth since A is, and likewise its fibers over S are geometrically connected. Thus, A/N is an abelian scheme as desired.

1.4.2.5. Theorem. *Let $\varphi : A \to B$ be an isogeny between abelian schemes over a scheme S, and let $N = \ker(\varphi)$. Duality applied to the exact sequence*

$$0 \to N \longrightarrow A \xrightarrow{\varphi} B \to 0$$

functorially yields an exact sequence

$$0 \to N^D \longrightarrow B^t \xrightarrow{\varphi^t} A^t \to 0.$$

That is, the map φ^t is an isogeny whose kernel is canonically isomorphic to N^D.

Moreover, double duality for abelian schemes and for finite locally free commutative group schemes are compatible up to a sign: if we identify φ and φ^{tt} via $\iota_{A/S}$ and $\iota_{B/S}$ then the natural isomorphism $(N^D)^D \simeq \ker((\varphi^t)^t) = \ker(\varphi^{tt}) \simeq \ker(\varphi) = N$ is the negative *of the canonical isomorphism provided by Cartier duality.*

We refer the reader to [**86**, Thm. 1.1, Cor. 1.3] for a proof based on arguments that relativize the ones over an algebraically closed field in [**82**]. (An alternative approach, at least for the first part, is [**87**, Thm. 19.1], resting on the link between dual abelian schemes and Ext-sheaves given in [**87**, Thm. 18.1].) The special case $\varphi = [n]_A : A \to A$ implies that naturally $A[n]^D = A^t[n]$ for every $n \geqslant 1$ because $[n]_A^t = [n]_{A^t}$ (by [**87**, 18.3]); this identification respects multiplicative change in n.

1.4.3. Constructions and definitions. Let us now focus on constructions specific to the theory of finite commutative group schemes over a perfect field k of characteristic $p > 0$. Let $W = W(k)$ be the ring of Witt vectors of k; e.g., if k is finite of size $q = p^r$ then W is the ring of integers in an unramified extension of $\mathbb{Q}_p$ of degree r. Let σ be the unique automorphism of W that reduces to the map $x \mapsto x^p$ on the residue field k.

1.4.3.1. Definition. The *Dieudonné ring* D_k over k is $W[\mathcal{F}, \mathcal{V}]$, where $\mathcal{F}$ and $\mathcal{V}$ are indeterminates subject to the relations

(1) $\mathcal{F}\mathcal{V} = \mathcal{V}\mathcal{F} = p$,
(2) $\mathcal{F}c = \sigma(c)\mathcal{F}$ and $c\mathcal{V} = \mathcal{V}\sigma(c)$ for all $c \in W$.

Explicitly, elements of D_k have unique expressions as finite sums

$$a_0 + \sum_{j>0} a_j \mathcal{F}^j + \sum_{j>0} b_j \mathcal{V}^j$$

with coefficients in W (so the center of D_k is clearly $\mathbb{Z}_p[\mathcal{F}^r, \mathcal{V}^r]$ if k has finite size p^r and it is $\mathbb{Z}_p$ otherwise; i.e., if k is infinite).

Some of the main conclusions in classical Dieudonné theory, as developed from scratch in [**41**, Ch. I–III], are summarized in the following theorem.

1.4.3.2. Theorem. *There is an additive anti-equivalence of categories $G \rightsquigarrow \mathrm{M}^*(G)$ from the category of finite commutative k-group schemes of p-power order to the category of left D_k-modules of finite W-length. Moreover, the following hold.*

(1) *A group scheme G has order $p^{\ell_W(\mathrm{M}^*(G))}$, where $\ell_W(\cdot)$ denotes W-length.*
(2) *If $k \to k'$ is an extension of perfect fields with associated extension $W \to W'$ of Witt rings (e.g., the absolute Frobenius automorphism of k) then the functor $W' \otimes_W (\cdot)$ on Dieudonné modules is naturally identified with the base-change*

functor on finite commutative group schemes. In particular, $\mathrm{M}^*(G^{(p)}) \simeq \sigma^*(\mathrm{M}^*(G))$ *as* W*-modules.*

(3) *Let* $\mathrm{Fr}_{G/k} : G \to G^{(p)}$ *be the relative Frobenius morphism. The* σ*-semilinear action on* $\mathrm{M}^*(G)$ *induced by* $\mathrm{M}^*(\mathrm{Fr}_{G/k})$ *through the isomorphism* $\mathrm{M}^*(G^{(p)}) \simeq \sigma^*(\mathrm{M}^*(G))$ *equals the action of* $\mathcal{F}$*, and* G *is connected if and only if* $\mathcal{F}$ *is nilpotent on* $\mathrm{M}^*(G)$*.*

(4) *There is a natural* k*-linear isomorphism* $\mathrm{M}^*(G)/\mathcal{F}\mathrm{M}^*(G) \simeq \mathrm{Lie}(G)^\vee$ *respecting extension of the perfect base field.*

(5) *For the Cartier dual* G^D*, naturally* $\mathrm{M}^*(G^D) \simeq \mathrm{Hom}_W(\mathrm{M}^*(G), K/W)$ *with* $K = W[1/p]$*, using the operators* $\mathcal{F}(\ell) : m \mapsto \sigma(\ell(\mathcal{V}(m)))$ *and* $\mathcal{V}(\ell) : m \mapsto \sigma^{-1}(\ell(\mathcal{F}(m)))$ *on* K/W*-valued linear forms* ℓ*.* □

For an abelian scheme $A \to S$ with fibers of constant dimension $g \geqslant 1$ and its finite commutative p^n-torsion subgroup scheme $A[p^n]$ with order $(p^n)^{2g}$, the directed system $A[p^\infty] := (A[p^n])_{n\geqslant 1}$ satisfies the following definition (with $h = 2g$).

1.4.3.3. Definition. A *p-divisible group of height* $h \geqslant 0$ over a scheme S is a directed system $G = (G_n)_{n\geqslant 1}$ of commutative S-groups G_n such that: G_n is killed by p^n, each $G_n \to S$ is finite and locally free, $[p]\colon G_{n+1} \to G_n$ is faithfully flat for every $n \geqslant 1$, $G_1 \to S$ has constant degree p^h, and G_n is identified with $G_{n+1}[p^n]$ for all $n \geqslant 1$.

The (Serre) *dual p-divisible group* G^t is the directed system (G_n^D) of Cartier dual group schemes G_n^D with the transition maps $G_n^D \to G_{n+1}^D$ that are Cartier dual to the quotient maps $[p] : G_{n+1} \to G_n$.

As an illustration, if $A \to S$ is an abelian scheme with fibers of dimension $g \geqslant 1$ then the isomorphisms $A[n]^D \simeq A^t[n]$ respecting multiplicative change in n (as noted immediately below Theorem 1.4.2.5) yield a canonical isomorphism between the Serre dual $A[p^\infty]^t$ and the p-divisible group $A^t[p^\infty]$ of the dual abelian scheme A^t (see [**86**, Prop. 1.8] or [**87**, Thm. 19.1]).

1.4.3.4. Remark. In view of the sign discrepancy for comparisons of double duality in Theorem 1.4.2.5, if $\varphi : A \to A^t$ is an S-homomorphism and

$$f : A[p^\infty] \to A^t[p^\infty] \simeq A[p^\infty]^t$$

is the associated homomorphism between p-divisible groups then the dual homomorphism $\varphi^t : A \to A^t$ (strictly speaking, $\varphi^t \circ \iota_{A/S}$ via double duality for abelian schemes) has as its associated homomorphism $A[p^\infty] \to A[p^\infty]^t$ the *negative*[1] of f^t (using double duality for p-divisible groups).

It follows that if φ is symmetric with respect to double duality for abelian schemes then f is skew-symmetric with respect to double duality for p-divisible groups. The converse is also true: we can see immediately via skew-symmetry of f that φ and φ^t induce the same homomorphism between p-divisible groups, and to conclude that $\varphi = \varphi^t$ it suffices to check on fibers due to the rigidity of abelian schemes (as in 1.4.2.2). On fibers we can apply the faithfulness of passage to p-divisible groups over fields via 1.2.5.1 with $\ell = p$.

[1] A related sign issue in the double duality for commutative finite group schemes over perfect fields is discussed in a footnote at the end of B.3.5.5.

1.4.3.5. Example. If $G = (G_n)$ is a p-divisible group over S (with height h) and $H = (H_n)$ is a p-divisible subgroup of G (with height $h' \leqslant h$) in the sense that H_n is a closed S-subgroup of G_n compatibly in n, then $G/H := (G_n/H_n)$ is also a p-divisible group over S. Indeed, a computation with fppf abelian sheaves shows that the complex

$$0 \to G_1/H_1 \to G_{n+1}/H_{n+1} \stackrel{[p]}{\to} G_n/H_n$$

is left exact in the sense of fppf abelian sheaves and hence the induced map

$$(G_{n+1}/H_{n+1})/(G_1/H_1) \to G_n/H_n$$

between finite locally free commutative S-groups is a closed immersion (as is any proper monomorphism), so it is an isomorphism for order reasons. This shows that the map $[p] : G_{n+1}/H_{n+1} \to G_n/H_n$ is faithfully flat with kernel G_1/H_1 of order $p^{h-h'}$, so induction on n implies that $(G_n/H_n)[p^m]$ is faithfully flat of order $p^{m(h-h')}$ for any $m \leqslant n$. In particular, the closed immersion $G_n/H_n \to (G_{n+1}/H_{n+1})[p^n]$ is an isomorphism for order reasons, so (G_n/H_n) is a p-divisible group.

In the preceding example, clearly the natural map $q : G \to G/H$ has functorial kernel H and has the mapping property of a quotient: any homomorphism of p-divisible groups $G \to G''$ that kills H uniquely factors through q. Hence, it is appropriate to define a *short exact sequence* of p-divisible groups to be a complex

$$0 \to G' \to G \to G'' \to 0$$

such that G' is a p-divisible subgroup of G and the induced map $G/G' \to G''$ is an isomorphism, or equivalently the induced complex of finite locally free commutative S-groups

$$0 \to G'_n \to G_n \to G''_n \to 0$$

is short exact for all $n \geqslant 1$.

For example, if $0 \to A' \to A \to A'' \to 0$ is a short exact sequence abelian schemes (in the sense of fppf abelian sheaves on the category of S-schemes), or equivalently $A \to A''$ is faithfully flat with kernel A', or equivalently it is short exact on geometric fibers over every point of S, then a computation with the snake lemma for fppf abelian sheaves shows that the induced complex

$$0 \to A'[p^\infty] \to A[p^\infty] \to A''[p^\infty] \to 0$$

is short exact. Also, by the definition of the Serre dual p-divisible group in terms of Cartier duality at finite levels, the Serre dual of a short exact sequence of p-divisible groups is short exact.

1.4.3.6. Example. An important example of a short exact sequence of p-divisible groups is the *connected-étale sequence* for a p-divisible group over a complete local noetherian ring R with residue characteristic $p > 0$. To define this, first recall that for any finite flat commutative R-group scheme H, the connected component H^0 of the identity section is an open and closed R-subgroup (in particular, it inherits R-flatness from H, so it is a finite flat R-group) and the associated finite flat quotient $H^{\text{ét}} := H/H^0$ is finite étale; these properties can be seen via the special fiber. The short exact sequence

$$0 \to H^0 \to H \to H^{\text{ét}} \to 0$$

of R-group schemes is the *connected-étale sequence* for H.

A p-divisible group $G = (G_n)$ over R is *connected* if each G_n is connected; equivalently, every G_n has infinitesimal special fiber. By a snake lemma argument with fppf abelian sheaves and the connected-étale sequence for finite flat commutative R-group schemes, if $G = (G_n)$ is a p-divisible group over R then $G^0 := (G_n^0)$ is a p-divisible group (called the *connected component* of G) and $G^{\text{ét}} := (G_n^{\text{ét}})$ is a p-divisible group (called the *étale part* of G). We call

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0$$

the *connected-étale sequence* for G.

Somewhat deeper lies the fact (see [**119**, §2.2] and [**75**, II, 3.3.18, 4.5]) that if G is a connected p-divisible group over R then $\mathcal{O}(G) := \varprojlim \mathcal{O}(G_n)$ is a formal power series ring in finitely many variables over R such that the induced formal R-group structure makes $[p]^* : \mathcal{O}(G) \to \mathcal{O}(G)$ finite flat, and moreover there is an equivalence

$$G \rightsquigarrow \widehat{G} := \mathrm{Spf}(\mathcal{O}(G))$$

from the category of connected p-divisible groups over R to the category of commutative formal Lie groups Γ over R for which $[p]_\Gamma$ is an isogeny. The quasi-inverse functor is $\Gamma \rightsquigarrow (\Gamma[p^n])$. This equivalence defines the (relative) *dimension* and *Lie algebra* for a connected p-divisible group over R, via analogous notions for formal Lie groups over R. By [**119**, §2.3, Prop. 3], $\dim(G) + \dim(G^t)$ is the height of G.

For later purposes, here is how this construction works in the important example of the p-divisible group $G = A[p^\infty]$ arising from an abelian R-scheme A. What is $\widehat{G}$? Let $\mathcal{C}_R$ denote the category of artinian local R-algebras that are module-finite over R (and hence killed by some power of the maximal ideal of R). Every point of A valued in such an algebra and supported at the identity of the special fiber is a point of the commutative formal Lie group $\widehat{A} := \mathrm{Spf}(\mathcal{O}_{A,0}^\wedge)$. A computation with formal group laws shows that all such points have p-power torsion, due to R having residue characteristic p. (This calculation will be given in a self-contained manner in the proof of Proposition 1.4.4.3.) Thus, for any $C \in \mathcal{C}_R$, the formal Lie group $\widehat{A}$ has each of its C-points supported in some $A[p^n]^0$. It follows that $\widehat{A}$ and $\widehat{G}$ pro-represent the same functor on $\mathcal{C}_R$, so the natural map $\widehat{G} \to \widehat{A}$ is an isomorphism. In particular, the p-divisible group of A has the same (relative) dimension and Lie algebra as A does.

1.4.3.7. Now consider p-divisible groups over a perfect field k of characteristic $p > 0$. For any p-divisible group $G = (G_n)_{n \geqslant 1}$ over k with height $h \geqslant 1$ we let $\mathrm{M}^*(G)$ denote the D_k-module $\varprojlim \mathrm{M}^*(G_n)$. By the same style of arguments used to work out the $\mathbb{Z}_\ell$-module structure of Tate modules of abelian varieties in characteristic $\neq \ell$ (resting on knowledge of the orders of the ℓ-power torsion subgroups), we use W-length to replace counting to infer that $\mathrm{M}^*(G)$ is a free W-module of rank h and

$$\mathrm{M}^*(G)/p^n\mathrm{M}^*(G) \to \mathrm{M}^*(G_n)$$

is an isomorphism for all $n \geqslant 1$. The p-divisible group G is connected if and only if $\mathcal{F}$ is topologically nilpotent on $\mathrm{M}^*(G)$ (since this is equivalent to the nilpotence of $\mathcal{F}$ on each $\mathrm{M}^*(G_n)$).

The Dieudonné module functor defines an anti-equivalence between the category of p-divisible groups over k (using the evident notion of morphism) and the category of left D_k-modules that are finite and free as W-modules; the W-rank of $\mathrm{M}^*(G)$ is equal to the height of G.

The notion of *isogeny* for p-divisible groups over a general scheme will be discussed in 3.3.3–3.3.5, but for our present purposes we only need the case when the base is a perfect field. This special case is easier to develop, and it is also convenient to have it available (on geometric fibers) when considering the relative case. Thus, we now define and briefly study this concept over perfect fields.

1.4.3.8. Definition. A homomorphism $f : X \to Y$ between p-divisible groups over a perfect field K is an *isogeny* if $\ker f$ is a finite K-group and the heights of X and Y coincide.

We first explain what this means in more concrete terms when $\mathrm{char}(K) \neq p$ by using p-adic Tate modules, and then the interesting case of perfect K of characteristic p will proceed similarly by using Dieudonné modules.

Assume $\mathrm{char}(K) \neq p$, so all p-divisible groups over K are étale (in the sense that each p^n-torsion subgroup is étale over K). Via the formation of p-adic Tate modules, the category of p-divisible groups over K is equivalent to the category of continuous linear representations of $\mathrm{Gal}(K_s/K)$ on finite free $\mathbb{Z}_p$-modules. It follows that f is an isogeny if and only if the induced map between p-adic Tate modules becomes an isomorphism after inverting p. Thus, a homomorphism $f : X \to Y$ between p-divisible groups is an isogeny if and only if there is a homomorphism $f' : Y \to X$ such that $f' \circ f = [p^n]_X$ and $f \circ f' = [p^n]_Y$ for some $n \geqslant 0$, and such an f is a quotient modulo the finite kernel $\ker(f)$ in the sense that any homomorphism of p-divisible groups $X \to X''$ over K that kills $\ker(f)$ factors uniquely through f.

By forming a quotient Tate module, we likewise see that for any finite K-subgroup $G \subset X$ there is an isogeny of p-divisible groups $f : X \to Y$ over K with $\ker(f) = G$, and f is unique up to unique isomorphism in an evident sense. We call Y the *quotient* of X modulo G and denote it as X/G. (It is not entirely trivial to describe $Y[p^n]$ in terms of X and G, and this will make the analogous construction over a general base scheme less straightforward.)

Now assume $\mathrm{char}(K) = p$ (and K is perfect). By arguing with Dieudonné modules in the role of p-adic Tate modules, it is elementary to check that a homomorphism $f : X \to Y$ between p-divisible groups over K is an isogeny if and only if the induced map $\mathrm{M}^*(f)$ between Dieudonné modules becomes an isomorphism after inverting p. Consequently, we again obtain that f is an isogeny if and only if there is a homomorphism $f' : Y \to X$ such that $f' \circ f = [p^n]_X$ and $f \circ f' = [p^n]_Y$ for some $n \geqslant 0$, and that f has the expected universal mapping property for homomorphisms from X that kill the finite kernel of f. Likewise, for any finite K-subgroup $G \subset X$ the induced map of (contravariant!) Dieudonné modules $\mathrm{M}^*(X) \to \mathrm{M}^*(G)$ is surjective (since $G \subset X[p^n]$ for large n), so the kernel of this surjection is W-finite free of the same rank as $\mathrm{M}^*(X)$. The corresponding p-divisible group is denoted X/G because the evident map $X \to X/G$ is an isogeny with kernel G.

As with abelian varieties, the *isogeny category* of p-divisible groups over a perfect field k of characteristic $p > 0$ is defined either by formally inverting isogenies or more concretely by using as the Hom-sets $\mathrm{Hom}^0(X, Y) = \mathrm{Hom}(X, Y)[1/p]$. For an abelian variety A of dimension $g > 0$ over k, the D_k-module $\mathrm{M}^*(A[p^\infty])$ is finite free of rank $2g$ over W, so it is an analogue of the ℓ-adic Tate module for $\ell \neq \mathrm{char}(k)$ even though it is contravariant in A. The D_k-module structure is the analogue of the Galois action on ℓ-adic Tate modules, though the action by $\mathcal{F}$ and $\mathcal{V}$ is highly non-trivial even when $k = \bar{k}$ (whereas the Galois action on Tate modules is trivial for such k). As an analogue of the Poincaré reducibility theorem for abelian varieties, the isogeny category of p-divisible groups over k is semisimple when $k = \overline{k}$; see Theorem 3.1.3. (This semisimplicity fails more generally, even over finite fields, as we see in the étale case: Galois groups can have non-semisimple representations on finite-dimensional $\mathbb{Q}_p$-vector spaces.)

To illustrate the use of Dieudonné modules as a replacement for Tate modules in the case $\ell = p$, we have the following result that will be important in our later study of a notion of "complex multiplication" for p-divisible groups.

1.4.3.9. Proposition. *Let G be a p-divisible group of height $h > 0$ over a field κ of characteristic p, and let k be a perfect extension of κ.*

1. *If F is a commutative semisimple $\mathbb{Q}_p$-subalgebra of $\mathrm{End}^0(G) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{End}(G)$ then $[F : \mathbb{Q}_p] \leqslant h$, with equality if and only if $\mathrm{M}^*(G_k)[1/p]$ is free of rank 1 as a $W(k) \otimes_{\mathbb{Z}_p} F$-module.*
2. *When equality holds, F is its own centralizer in $\mathrm{End}^0(G)$. If moreover the maximal $\mathbb{Z}_p$-order $\mathcal{O}_F$ in F lies in $\mathrm{End}(G)$ then $\mathrm{M}^*(G_k)$ is free of rank 1 as a $W(k) \otimes_{\mathbb{Z}_p} \mathcal{O}_F$-module.*

In 3.1.8 we will show that $\mathrm{End}(G)$ is finitely generated as a $\mathbb{Z}_p$-module, but this fact is not needed here.

Proof. We may and do replace κ with k, so κ is perfect. (In particular, we may use the notion of isogeny as in 1.4.3.8.) Letting $K_0 = W(\kappa)[1/p]$, we view $\mathrm{M}^*(G)[1/p]$ as a finite module over the semisimple ring $K_0 \otimes_{\mathbb{Q}_p} F$. The second condition in (2) is immediate from the freeness in (1) (as $W(\kappa) \otimes_{\mathbb{Z}_p} \mathcal{O}_F$ is a finite product of discrete valuation rings that are $W(\kappa)$-finite, and $\mathrm{M}^*(G)$ is finite free as a $W(\kappa)$-module), so it is harmless to pass to an F-linearly isogenous p-divisible group. Thus, we may decompose G according to the idempotents of F to reduce to the case when F is a p-adic field. Let k_0 be its finite residue field, $F_0 = W(k_0)[1/p]$, κ' a compositum of k_0 with κ over $\mathbb{F}_p$, and $K_0' = W(\kappa')[1/p]$. Consider the decomposition

$$K_0 \otimes_{\mathbb{Q}_p} F = (K_0 \otimes_{\mathbb{Q}_p} F_0) \otimes_{F_0} F \simeq \prod_{j : k_0 \to \kappa'} (K_0' \otimes_{j, F_0} F)$$

where j varies through the embeddings over $k_0 \cap \kappa$ ($\subset k_0$). This is a finite product of copies of totally ramified finite extensions of K_0', and the factor fields are permuted transitively by the natural F-linear action of the Galois group $\mathrm{Gal}(k_0/(k_0 \cap \kappa))$. Note that this Galois group is generated by a power of the absolute Frobenius.

We conclude that any $K_0 \otimes_{\mathbb{Q}_p} F$-module M canonically decomposes in a compatible F-linear way as $\prod M_j$ for vector spaces M_j over the factors fields. Hence, if M is equipped with an injective F-linear endomorphism $\mathcal{F}$ that is semilinear over the absolute Frobenius of K_0' then $\mathcal{F}$ must be an F-linear automorphism that transitively permutes the M_j's via F-linear isomorphisms. In particular, if such an M is non-zero then each M_j is a non-zero vector space over the factor field indexed by j, so M as a $K_0 \otimes_{\mathbb{Q}_p} F$-module would be free of some positive rank ρ and hence of K_0-dimension $[F : \mathbb{Q}_p]\rho$.

Now set $M = \mathrm{M}^*(G)[1/p]$, whose K_0-dimension is h. This is equipped with the required Frobenius-semilinear injective endomorphism (that is moreover F-linear by functoriality), so it is free of some rank $\rho \geqslant 1$ over $K_0 \otimes_{\mathbb{Q}_p} F$ and hence $h = [F : \mathbb{Q}_p]\rho$. It follows that $[F : \mathbb{Q}_p] \leqslant h$, with equality if and only if $\rho = 1$. This proves (1).

Finally, assuming we are in this rank-1 case, it remains to prove that F is its own centralizer in $\mathrm{End}^0(G)$. To compute the centralizer of F, first observe that the Dieudonné module functor (on the isogeny category) is valued in the category of K_0-vector spaces, so every element $f \in \mathrm{End}^0(G)$ that commutes with the F-action induces a $K_0 \otimes_{\mathbb{Q}_p} F$-linear endomorphism of $\mathrm{M}^*(G)[1/p]$. We know that $\mathrm{M}^*(G)[1/p]$ is free of rank 1 over $K_0 \otimes_{\mathbb{Q}_p} F$, so $\mathrm{M}^*(f)$ acts as multiplication by some $c \in K_0 \otimes_{\mathbb{Q}_p} F$. Since $\mathrm{M}^*(f)$ also commutes with the action of $\mathcal{F}$ that is semilinear over the absolute Frobenius σ of K_0, we have $(\sigma \otimes 1)(c) = c$. This forces $c \in F$, as desired. □

1.4.4. Deformation theory. Let R be a local ring with residue field κ. The functor $A \rightsquigarrow A_\kappa$ from abelian schemes over R to abelian varieties over κ is faithful. This follows from two facts: the collection of finite étale subgroup schemes $A[N]$ for N not divisible by $\mathrm{char}(\kappa)$ is schematically dense in A (due to the fiberwise denseness and [**34**, IV_3, 11.10.9]), and passage to the special fiber is faithful on finite étale R-schemes. When considering deformation problems for abelian varieties equipped with endomorphisms or a polarization (viewed as a special kind of isogeny), this faithfulness result is implicitly used without comment.

1.4.4.1. Remark. For abelian R-schemes A and B, the injective reduction map

$$\mathrm{Hom}^0(A, B) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(A, B) \to \mathrm{Hom}^0(A_\kappa, B_\kappa)$$

gives meaning to the intersection $\mathrm{Hom}^0(A, B) \bigcap \mathrm{Hom}(A_\kappa, B_\kappa)$. This intersection contains $\mathrm{Hom}(A, B)$ but can be strictly larger. To make an example, let R be a discrete valuation ring with fraction field K of characteristic 0 and residue field κ of characteristic $p > 0$, and let E be an elliptic curve over R such that $E[p]_K$ is constant and E_κ is ordinary. There are $p+1$ cyclic subgroups of $E[p]_K$ with order p, so via R-flat closure there are $p+1$ closed R-flat subgroups $C \subset E$ of order p. For any local extension of discrete valuation rings $R \hookrightarrow R'$, the R'-subgroups $\{C_{R'}\}$ of $E_{R'}$ exhaust the $p+1$ possibilities over R'. Due to the connected-étale sequence over $\widehat{R}$, it follows that exactly one such $C \subset E$ is connected, so the p others are étale and hence have reduction equal to the same (unique) étale κ-subgroup of $E_\kappa[p]$.

If $C, C' \subset E[p]$ are distinct étale subgroups of order p then the kernels of the isogenies $f : E \to E/C$ and $f' : E \to E/C'$ are distinct over K but the same over κ. Since the reductions of f and f' have the same kernel, in the isogeny category of elliptic curves over R the element $f \circ (f')^{-1} \in \mathrm{Hom}^0(E/C', E/C)$ has reduction that is a morphism of elliptic curves (and even an isomorphism, with inverse given by the reduction of $f' \circ f^{-1}$). If $f \circ f'^{-1}$ were a morphism of elliptic curves over R then it would have to be an isomorphism (since its reduction is an isomorphism), and so C' would be in the orbit of C under $\mathrm{Aut}(E) = \mathrm{Aut}(E_K)$. These orbits have size at most $\#\mathrm{Aut}(E_K)/2 \leqslant 3$, so we can find C' and C not in the same $\mathrm{Aut}(E)$-orbit whenever $j(E_K) \neq 0, 1728$ or $p > 3$.

The analogous faithfulness result for p-divisible groups is more subtle when $\mathrm{char}(\kappa) = p$, since it is false without a noetherian condition:

1.4.4.2. Example. Let $R = \mathbb{Z}_p[\zeta_{p^\infty}]$ be the (non-noetherian) valuation ring of the p-power cyclotomic extension of $\mathbb{Q}_p$, and let $\{\zeta_{p^n}\}$ a compatible system of primitive p-power roots of unity in R. The R-homomorphism between p-divisible groups $\mathbb{Q}_p/\mathbb{Z}_p \to \mu_{p^\infty}$ defined by $p^{-n} \mapsto \zeta_{p^n}$ is an isomorphism between the generic fibers and induces the zero map between the special fibers.

Under a noetherian hypothesis, the preceding pathology cannot occur:

1.4.4.3. Proposition. *Let $(R, \mathfrak{m})$ be a noetherian local ring with residue field κ of characteristic $p > 0$. The functor $G \rightsquigarrow G_\kappa$ from p-divisible groups over R to p-divisible groups over κ is faithful.*

Proof. The problem is to prove that if $f : G' \to G$ is a homomorphism between p-divisible groups over R and $f_\kappa = 0$ then $f = 0$. For each $n \geqslant 1$, the induced map $f_n : G'[p^n] \to G[p^n]$ between finite flat R-group schemes is described by a matrix over R upon choosing R-bases of the coordinate rings (as finite free R-modules). Hence, by the Krull intersection theorem it suffices to prove the vanishing result over $R/\mathfrak{m}^N$ for all $N \geqslant 1$, so we may and do assume that R is an artinian local ring. By the functoriality of the connected-étale sequence, it suffices to treat the following separate cases: G' and G are both connected, G' and G are both étale, or G' is étale and G is connected.

The case when both are étale is obvious. When G' is étale and G is connected then we claim that $\mathrm{Hom}(G', G) = 0$. By faithfully flat base change to the (artinian local) strict henselization R^{sh} we may assume G' is constant, so it is a power of $\mathbb{Q}_p/\mathbb{Z}_p$. Hence, we can assume $G' = \mathbb{Q}_p/\mathbb{Z}_p$, so $\mathrm{Hom}(G', G) = \varprojlim G[p^n](R)$ (inverse limit via p-power maps). The equivalence between connected p-divisible groups and formal Lie groups over R on which multiplication by p is an isogeny (see Example 1.4.3.6) identifies this inverse limit with the p-adic Tate module of $\widehat{G}(R)$, where $\widehat{G}$ is the formal Lie group associated to G. Hence, the desired vanishing is reduced to proving that $\widehat{G}(R)$ has no non-zero infinitely p-divisible elements. In fact, we claim that $[p^N]$ kills $\widehat{G}(R)$ for sufficiently large N.

Upon choosing formal parameters for $\widehat{G}$, we may identify the set $\widehat{G}(R)$ with the set of ordered d-tuples in $\mathfrak{m}$, where $d = \dim G$. If $g \in \widehat{G}(R)$ has coordinates in an ideal I of R then $[p](g)$ has coordinates in (pI, I^2) since $[p]$ has linear part given by p-multiplication on the coordinates. Hence, if we define the sequence of ideals $J_0 = \mathfrak{m}$ and $J_{n+1} = (pJ_n, J_n^2)$ then we just need $J_N = 0$ for sufficiently large N. More generally, for any ring whatsoever and any ideal J_0, an elementary induction argument shows that $J_n \subset (p, J_0)^n$. The nilpotence of $\mathfrak{m}$ then does the job.

Finally, we address the most interesting case, which is connected G' and G. In this case we switch to the perspective of formal Lie groups and aim to prove that for commutative formal Lie groups Γ and Γ' over R such that $[p]_{\Gamma'}$ is an isogeny, $\mathrm{Hom}(\Gamma', \Gamma) \to \mathrm{Hom}(\Gamma'_\kappa, \Gamma_\kappa)$ is injective. Consider $f \in \mathrm{Hom}(\Gamma, \Gamma')$ that vanishes modulo an ideal $I \subseteq \mathfrak{m}$. Choose formal coordinates $\{x'_i\}$ and $\{x_j\}$ for Γ' and Γ respectively, so the coefficients of all monomials in $f^*(x_j)$ lie in I. Hence, the formal power series $(f \circ [p]_{\Gamma'})^*(x_j) = [p]^*_{\Gamma'}(f^*(x_j))$ has all coefficients of all monomials lying in (pI, I^2). Iterating, if $f \in \mathrm{Hom}(\Gamma', \Gamma)$ vanishes over κ then $f \circ [p^n]_{\Gamma'}$ vanishes modulo the ideal J_n, where $J_0 = \mathfrak{m}$ and $J_{n+1} = (pJ_n, J_n^2)$. We have already seen that $J_N = 0$ for sufficiently large N, so $f \circ [p^N]_{\Gamma'} = 0$ for large N. By hypothesis the isogenous endomorphism $[p^N]_{\Gamma'} = [p]_{\Gamma'}^N$ of Γ' induces an injective endomorphism of the coordinate ring, so $f = 0$. □

An important fact in the study of lifting problems for abelian varieties from characteristic p to characteristic 0 is that infinitesimal lifting for such an abelian variety is entirely controlled by that of its p-divisible group. This will be made precise in Theorem 1.4.5.3 (and Example 1.4.5.4 will address algebraization aspects in the limit). We now focus on the existence and structure of deformation rings for abelian varieties and p-divisible groups as well as the behavior of these deformation rings relative to extension of the residue field.

1.4.4.4. Definition. Let A_0 be an abelian variety of dimension g over a field κ. For a complete local noetherian ring R with residue field κ, a *deformation* of A_0 over R is a pair (A, i) consisting of an abelian scheme A over R and an isomorphism $i : A_\kappa \simeq A_0$ over κ.

There is an evident notion of *isomorphism* between two deformations of A_0 over R, and such deformations have no non-trivial automorphisms. Likewise, if A_0 is equipped with a polarization $\phi_0 : A_0 \to A_0^t$ or an injective homomorphism $\alpha_0 : \mathcal{O} \to \mathrm{End}(A_0)$ from a specified $\mathbb{Z}$-finite associative ring $\mathcal{O}$ (or both!), we define in an evident way the notion of *deformation* for A_0 equipped with this additional structure. In the case of polarizations, any R-homomorphism $\phi : A \to A^t$ lifting ϕ_0 is necessarily a polarization. Indeed, the symmetry of ϕ is inherited from ϕ_0 (due to faithfulness of passage to the special fiber for abelian schemes over a local ring), and the ampleness on A of the pullback $(1, \phi)^*(\mathscr{P}_A)$ of the Poincaré bundle $\mathscr{P}_A$ is inherited from the ampleness on A_0 of its restriction $(1, \phi_0)^*(\mathscr{P}_{A_0})$ due to [**34**, IV$_3$, 9.6.4].

Fix a complete local noetherian ring Λ with residue field κ (e.g., a Cohen ring for κ), and let $\mathcal{C}_\Lambda$ be the category of artinian local Λ-algebras R with local structure map $\Lambda \to R$ and residue field κ. The *deformation functor*

$$\mathrm{Def}_\Lambda(A_0) : \mathcal{C}_\Lambda \to \mathrm{Set}$$

assigns to every R in $\mathcal{C}_\Lambda$ the set of isomorphism classes of deformations of A_0 over R. Likewise, if A_0 is equipped with a polarization $\phi_0 : A_0 \to A_0^t$ and endomorphism structure $\alpha_0 : \mathcal{O} \hookrightarrow \mathrm{End}(A_0)$ (for a $\mathbb{Z}$-finite associative ring $\mathcal{O}$) then we define the deformation functor $\mathrm{Def}_\Lambda(A_0, \phi_0, \alpha_0)$ similarly. This is a subfunctor of $\mathrm{Def}_\Lambda(A_0)$.

A covariant functor $F : \mathcal{C}_\Lambda \to \mathrm{Set}$ is *pro-representable* if there is a complete local noetherian Λ-algebra $\mathcal{R}$ with local structure map $\Lambda \to \mathcal{R}$ and residue field κ such that $F \simeq \mathrm{Hom}_\Lambda(\mathcal{R}, \cdot)$ (using local Λ-algebra homomorphisms). A *formal deformation ring* for A_0 (if one exists) is an $\mathcal{R}$ that pro-represents $\mathrm{Def}_\Lambda(A_0)$. The reason we say "formal" is that over such an $\mathcal{R}$ there is merely a universal *formal* abelian scheme (which is however universal modulo $\mathfrak{m}_{\mathcal{R}}^n$ among abelian scheme deformations of A_0 over objects in $\mathcal{C}_\Lambda$ whose maximal ideal has vanishing nth power, for each $n \geqslant 1$).

When we include a polarization as part of the deformation problem, if this enhanced problem admits a pro-representing ring $\mathcal{R}$ then by Grothendieck's formal

GAGA algebraization theorems [**34**, III_1, 5.4.1, 5.4.5] there is a universal deformation (i.e., a polarized abelian scheme deformation over $\mathcal{R}$ that represents the deformation functor on the category of all complete local noetherian Λ-algebras with residue field κ).

1.4.4.5. Theorem. *The deformation functor* $\mathrm{Def}_\Lambda(A_0)$ *is pro-representable and formally smooth, with tangent space canonically isomorphic to* $\mathrm{Lie}(A_0^t) \otimes_\kappa \mathrm{Lie}(A_0)$ *as a* κ*-vector space. In particular, this formal deformation ring is a formal power series ring over* Λ *in* g^2 *variables.*

Each deformation functor $\mathrm{Def}_\Lambda(A_0, \phi_0, \alpha_0)$ *and* $\mathrm{Def}_\Lambda(A_0, \alpha_0)$ *is pro-represented by a quotient of the formal deformation ring for* A_0*.*

PROOF. The case of $\mathrm{Def}_\Lambda(A_0)$ is due to Grothendieck and is explained in detail in [**88**, Thm. 2.2.1] (where the description of the tangent space to the deformation functor is given in the proof). To show that a deformation functor F of the form $\mathrm{Def}_\Lambda(A_0, \phi_0, \alpha_0)$ or $\mathrm{Def}_\Lambda(A_0, \alpha_0)$ is pro-represented by a quotient of the formal deformation ring $(\mathcal{R}, \mathfrak{m})$ for A_0, for each integer $n \geqslant 1$ we consider the full subcategory $\mathcal{C}_{\Lambda,n}$ of objects $R \in \mathcal{C}_\Lambda$ whose maximal ideal has vanishing nth power. The restriction $\mathrm{Def}_\Lambda(A_0)|_{\mathcal{C}_{\Lambda,n}}$ is represented by $\mathcal{R}/\mathfrak{m}^n$. For each n, suppose there is an ideal $I_n \subset \mathcal{R}/\mathfrak{m}^n$ such that $(\mathcal{R}/\mathfrak{m}^n)/I_n$ represents the subfunctor $F|_{\mathcal{C}_{\Lambda,n}}$ of $\mathrm{Def}_\Lambda(A_0)|_{\mathcal{C}_{\Lambda,n}}$. Since $\mathcal{C}_{\Lambda,n}$ is a full subcategory of $\mathcal{C}_{\Lambda,n+1}$, by universality we see that I_{n+1} has image I_n under $\mathcal{R}/\mathfrak{m}^{n+1} \to \mathcal{R}/\mathfrak{m}^n$. Hence, there is a unique ideal $I \subset \mathcal{R}$ such that $I_n = (I + \mathfrak{m}^n)/\mathfrak{m}^n$ for all $n \geqslant 1$, so $\mathcal{R}/I$ is the desired quotient.

We are reduced to the following general problem for abelian schemes (applied to the universal deformation of A_0 over $\mathcal{R}/\mathfrak{m}^n$ for every $n \geqslant 1$ and the structure (ϕ_0, α_0) on its reduction A_0 modulo the nilpotent ideal $\mathfrak{m}/\mathfrak{m}^n$). Let A and B be abelian schemes over a noetherian scheme S, and let $\mathscr{I} \subset \mathcal{O}_S$ be a nilpotent coherent ideal sheaf defining a closed subscheme $S_0 \subset S$. For a homomorphism $f_0 : A_0 \to B_0$ over S_0, the condition on an S-scheme T that $(f_0)_{T_0}$ lifts (necessarily uniquely!) to a T-homomorphism $A_T \to B_T$ is represented by a closed subscheme of S (visibly containing S_0). We will prove this by using Hom-schemes.

Consider the functor $\underline{\mathrm{Hom}}(A, B) : T \rightsquigarrow \mathrm{Hom}_{T\text{-gp}}(A_T, B_T)$ on S-schemes. We shall prove this is represented by an S-scheme locally of finite type (avoiding projectivity hypotheses on A and B). Grothendieck's construction of Hom-schemes from Hilbert schemes (via graph arguments) for schemes that are proper, flat, and finitely presented over the base requires projectivity because this hypothesis is needed to ensure representability of Hilbert functors. But Artin showed (see [**5**, Cor. 6.2]) that the Hilbert functor of a proper, flat, and finitely presented S-scheme X is an algebraic space that is separated and locally of finite type over S. Consequently, the same holds for Hom-functors between such schemes, and so also for the subfunctors that impose compatibility with group laws.

We conclude that $H := \underline{\mathrm{Hom}}(A, B)$ is an algebraic space that is separated and locally of finite type over S. For all $s \in S$ the fibers H_s are étale (by the functorial criterion), and an algebraic space that is separated and locally quasi-finite over a noetherian scheme is a scheme [**60**, II, 6.16]. Thus, H is represented by a separated and locally finite type S-scheme that we denote also as H.

The given f_0 defines a section to $H_0 := H \times_S S_0 \to S_0$. We claim that the closed subscheme $Z_0 \hookrightarrow H_0$ underlying this section is stable under generization. Suppose not, so there exists a discrete valuation ring R and an element $h_0 \in H_0(R)$ whose generic point lands outside Z_0 and whose closed point lands inside Z_0. Making a base change by the resulting map $\mathrm{Spec}(R) \to S_0$ yields a pair of R-homomorphisms $(A_0)_R \rightrightarrows (B_0)_R$ (one coming from h_0, and the other from f_0) that agree on the closed fibers but are distinct on generic fibers, contradicting faithfulness of passage to the special fiber for abelian schemes over a local ring.

By stability under generization, the closed subscheme Z_0 in H_0 is topologically open, so the open subscheme $U \subset H$ with the underlying space of Z_0 is a union of connected components of H. The structure morphism $U \to S$ is a homeomorphism, so it is of finite type, not just locally of finite type. The map $H \to S$ satisfies the valuative criterion for properness since an abelian scheme over a discrete valuation ring is the Néron model of its generic fiber [**10**, 1.2/8], so the open and closed U in H also satisfies the valuative criterion over S. This proves that the finite type map $U \to S$ is proper, yet it has étale fibers of degree 1, so it is a closed immersion (defined by a nilpotent ideal). The closed subscheme $U \hookrightarrow S$ represents the lifting condition on f_0. □

1.4.4.6. Remark. A globalization of the formal smoothness of the infinitesimal deformation theory of an abelian variety is Grothendieck's result that if R is a ring containing an ideal J satisfying $J^2 = 0$ then every abelian scheme A_0 over $R_0 := R/J$ lifts to an abelian scheme over R. We sketch the proof, building on the key case of an artinian local base that follows from the formal smoothness of the infinitesimal deformation theory (and is a key step in the *proof* of the formal smoothness in [**88**, Thm. 2.2.1]).

By direct limit arguments we may and do assume R is noetherian. The obstruction to lifting A_0 to a smooth proper R-scheme A is a certain class $\xi \in \mathrm{H}^2(A_0, (\Omega^1_{A_0/R_0})^\vee \otimes_{R_0} J)$. The formation of ξ is compatible with base change on R (relative to base change morphisms for the cohomology of quasi-coherent sheaves), so by Zariski localization and completion we see that the vanishing of ξ is reduced to the case when R is a complete local noetherian ring. By the Theorem on Formal Functions [**34**, III_1, 4.2.1], the vanishing of ξ is reduced to the settled case when R is an artinian local ring.

Now return to a general noetherian R, and fix a smooth proper R-scheme A lifting A_0. By smoothness we may choose a lift $e \in A(R)$ of the identity section $e_0 \in A_0(R_0)$. We claim that the subtraction morphism $\mu_0 : A_0 \times A_0 \to A_0$ defined by $(x, y) \mapsto x - y$ uniquely lifts to an R-morphism $\mu : A \times A \to A$ carrying (e, e) to e. Once such a μ exists, it is the subtraction for a unique group law due to rigidity arguments explained in [**83**, Ch. 6, §3]. In particular, over an arbitrary ring R (without noetherian hypotheses) μ is unique if it exists. Hence, by Zariski localization it suffices to prove the existence of μ when R is a local noetherian ring, and by fpqc descent with respect to $R \to \widehat{R}$ we may assume R is complete. Formal GAGA for morphisms [**83**, III_1, 5.4.1] then reduces the existence problem to the case of artinian local R, so by length induction we may assume J is killed by the maximal ideal of R. This case is settled in [**83**, Ch. 6, §3, Prop. 6.15].

The deformation theory of p-divisible groups ends up with results similar to the case of abelian varieties but proceeds by another path. To describe this, let κ be a field of characteristic $p > 0$, Λ a complete local noetherian ring with residue field κ, and X_0 a p-divisible group of height $h \geqslant 0$ and dimension $d \geqslant 0$ over κ (so

$\dim(X_0^t) = h - d$ by [**119**, §2.3, Prop. 3]). A *deformation* of X_0 over a complete local noetherian ring R with residue field κ is a pair $(\mathcal{X}, i)$ consisting of a p-divisible group $\mathcal{X}$ over R and an isomorphism $i : \mathcal{X}_\kappa \simeq X_0$.

There is an evident notion of *morphism* between such pairs. By Proposition 1.4.4.3, deformations of X_0 have no non-trivial automorphisms (lifting the identity on X_0). Hence, it is reasonable to study the functor $\mathrm{Def}_\Lambda(X_0)$ assigning to any $R \in \mathcal{C}_\Lambda$ the set of isomorphism classes of deformations of X_0 over R. In contrast with the deformation theory of non-zero abelian varieties, for which the universal formal deformation is never algebraizable beyond the case of elliptic curves, the universal formal deformation of a p-divisible group is also a universal deformation relative to all complete local noetherian Λ-algebras with residue field κ since p-divisible groups are built from torsion-levels that are *finite* flat over the base.

1.4.4.7. Theorem. *The functor* $\mathrm{Def}_\Lambda(X_0)$ *is pro-represented by a power series ring over* Λ *in* $d(h-d)$ *variables. The tangent space* t_{X_0} *to this functor is canonically isomorphic to* $\mathrm{Lie}(X_0^t) \otimes_\kappa \mathrm{Lie}(X_0)$ *as a* κ*-vector space.*

The pro-representability for connected X_0 over perfect κ is established in [**124**] by using formal group laws to verify Schlessinger's criteria; the perfectness is required to carry out a Dieudonné module computation establishing that $\dim_\kappa(t_{X_0}) < \infty$ (equal to $d(h-d)$). This approach does not prove formal smoothness. Over algebraically closed fields the pro-representability for general X_0 is deduced formally from the connected case in the proof of [**16**, Thm. 4.4 (2)]. The general case over any κ may be deduced from Schlessinger's criteria and [**51**, 4.4]; the latter ingredient is proved via the cotangent complex (also see [**51**, 4.8] for perfect κ). For the convenience of the reader, here is a proof for general κ that avoids the machinery of the cotangent complex.

PROOF. First, we address the formal smoothness. The case of connected X_0 is a special case of the unobstructedness of lifting commutative formal Lie groups, which can be proved over any ring via Cartier theory; see [**136**, Thm. 4.46]. For disconnected X_0 consider a deformation X of X_0 over an artinian local Λ-algebra R with residue field κ. There is a unique (up to unique isomorphism) étale p-divisible group E over R that lifts $X_0^{\text{ét}}$ over κ, so $X^{\text{ét}}$ is uniquely isomorphic to E as deformations of $X_0^{\text{ét}}$.

Since X^0 is a deformation of the identity component of X_0, we see that the construction of such X comes in two steps: (i) deform X^0 to a (necessarily connected) p-divisible group over R (this step is unobstructed, by the settled connected case), and (ii) construct extensions over R of E by the chosen deformation of X_0^0. Such extensions in the sense of fppf abelian sheaves on the category $\mathscr{C}_R$ of finite R-algebras (equipped with the fppf topology) arise from p-divisible groups, due to:

1.4.4.8. Lemma. *Let* R *be an local artinian ring with residue characteristic* $p > 0$*, and choose a connected* p*-divisible group* G *over* R *and an étale* p*-divisible group* E *over* R*. For any short exact sequence of fppf abelian sheaves*

$$0 \to G \to Y \to E \to 0 \qquad (1.4.4.1)$$

on the category $\mathscr{C}_R$ *of finite* R*-algebras* (*with the fppf topology*)*,* Y *is a* p*-divisible group* (*so the given short exact sequence is the connected-étale sequence of* Y)*.*

PROOF. Since G and E are p-power torsion sheaves, the sheaf Y is the union of its subsheaves $Y[p^n]$ for $n \geqslant 1$. The snake lemma gives that $[p] : Y \to Y$ is an epimorphism and provides short exact sequences of abelian sheaves

$$0 \to G[p^n] \to Y[p^n] \to E[p^n] \to 0$$

for all $n \geqslant 1$. The outer terms are represented by finite flat R-group schemes, so by Proposition 1.4.1.3 the middle term must also be represented by a finite flat R-group scheme. Thus, Y is a p-divisible group. □

Over any base scheme S, the study of extensions of an étale p-divisible group E by a given p-divisible group G over S can be reduced to the special case $E = \mathbb{Q}_p/\mathbb{Z}_p$ at the cost of replacing G with a p-divisible group denoted $E^\vee \otimes G$, as follows.

Let $E^\vee \otimes G$ be the direct limit (over $n \to \infty$) of the tensor products

$$E[p^n]^\vee \otimes_{\mathbb{Z}/(p^n)} G[p^n]$$

of $G[p^n]$ against the $\mathbb{Z}/(p^n)$-linear dual $E[p^n]^\vee$ of the étale sheaf $E[p^n]$, using the evident transition maps. This is easily seen to be a p-divisible group. Note that if S is the spectrum of a complete local noetherian ring with residue characteristic p and if G is connected then $E^\vee \otimes G$ is connected with dimension $\mathrm{height}(E) \cdot \dim(G)$.

There is a general categorical equivalence (compatible with base change) from the category of extensions of E by G to the category of extensions of the constant p-divisible group $\mathbb{Q}_p/\mathbb{Z}_p$ by $E^\vee \otimes G$. In one direction, for an extension (1.4.4.1) apply $E^\vee \otimes (\cdot)$ and then pull back the short exact sequence

$$0 \to E^\vee \otimes G \to E^\vee \otimes Y \to E^\vee \otimes E \to 0$$

along $\mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow E^\vee \otimes E$ corresponding to the identity map in $E[p^n]^\vee \otimes E[p^n] = \mathscr{E}nd(E[p^n])$ for $n \geqslant 1$. In the other direction, given an extension of $\mathbb{Q}_p/\mathbb{Z}_p$ by $E^\vee \otimes G$, we apply $E \otimes (\cdot)$ to the given exact sequence and push out along the evaluation map $E \otimes E^\vee \otimes G \to G$. In an evident way, these are quasi-inverse constructions.

To summarize, the formal smoothness of $\mathrm{Def}_\Lambda(X_0)$ for disconnected X_0 is reduced to cases with $X_0^{\text{ét}} = \mathbb{Q}_p/\mathbb{Z}_p$. Since the deformation theory is formally smooth in the connected case, the formal smoothness of $\mathrm{Def}_\Lambda(X_0)$ is reduced to the following assertion.

1.4.4.9. Lemma. *Let $(R, \mathfrak{m})$ be artinian local with residue field κ of characteristic $p > 0$, J a non-zero ideal in R such that $\mathfrak{m}J = 0$, and $R_0 := R/J$. For a connected p-divisible group G over R with reduction G_0 over R_0,*

$$\mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, G) \to \mathrm{Ext}^1_{R_0}(\mathbb{Q}_p/\mathbb{Z}_p, G_0)$$

is surjective.

PROOF. As above, let $\mathscr{C}_R$ denote the category of finite R-algebras, equipped with the fppf topology, and define $\mathscr{C}_{R_0}$ similarly; the Ext-groups are computed in the categories of abelian fppf sheaves on the respective sites $\mathscr{C}_R$ and $\mathscr{C}_{R_0}$. By writing $\mathbb{Q}/\mathbb{Z}$ as the direct sum of its p-primary part $\mathbb{Q}_p/\mathbb{Z}_p$ and its prime-to-p part M,

$$\mathrm{Ext}^1_R(\mathbb{Q}/\mathbb{Z}, G) = \mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, G) \oplus \mathrm{Ext}^1_R(M, G).$$

The final Ext-term vanishes: any extension E of M by G is a torsion sheaf, so the decomposition of E as a direct sum of its p-primary part and prime-to-p part splits the extension structure. Thus, our problem is proving the surjectivity of

$$\mathrm{Ext}^1_R(\mathbb{Q}/\mathbb{Z}, G) \to \mathrm{Ext}^1_{R_0}(\mathbb{Q}/\mathbb{Z}, G_0).$$

Consider the evident commutative diagram of long exact sequences

$$\begin{array}{ccccccccc} 0 & \to & G(R) & \to & \mathrm{Ext}^1_R(\mathbb{Q}/\mathbb{Z}, G) & \to & \mathrm{Ext}^1_R(\mathbb{Q}, G) & \to & \mathrm{H}^1(R, G) \\ & & \downarrow & & \downarrow f & & \downarrow f' & & \downarrow f'' \\ 0 & \to & G_0(R_0) & \to & \mathrm{Ext}^1_{R_0}(\mathbb{Q}/\mathbb{Z}, G_0) & \to & \mathrm{Ext}^1_{R_0}(\mathbb{Q}, G_0) & \to & \mathrm{H}^1(R_0, G_0) \end{array}$$

We want f to be surjective. The functor G on $\mathscr{C}_R$ is pro-represented by the coordinate ring $\mathcal{O}(G)$ of the associated formal Lie group, so it is formally smooth. Hence, the left vertical map is surjective, so by the 5-lemma it suffices to show that f' is surjective and f'' is injective.

We first show that f'' is injective, for which it suffices to show that any G-torsor fppf sheaf of sets X on $\mathscr{C}_R$ is formally smooth. There is a local finite flat cover R' of R such that $X|_{\mathscr{C}_{R'}}$ is pro-represented by $\mathcal{O}(G)_{R'}$, so X is pro-represented by an R-descent A of $\mathcal{O}(G)_{R'}$; this descent is easily checked to be a complete noetherian local R-algebra (and its functor on $\mathscr{C}_R$ is computed using local ring homomorphisms). Clearly A is R-flat and the scalar extension $\kappa' \otimes_\kappa A_\kappa$ over the residue field κ' of R' is a formal power series ring over κ'. It follows that $k \otimes_\kappa A_\kappa$ is regular for any finite extension k of κ (it suffices to consider k containing κ', as a noetherian ring with a regular faithfully flat extension is regular [**73**, Thm. 23.7]), so A_κ is "geometrically regular" over κ. Thus, A_κ is formally smooth over κ relative to its max-adic topology [**73**, Thm. 28.7], so R-flatness ensures that A is formally smooth over R relative to its max-adic topology by [**34**, 0_{IV}, 19.7.1].

It remains to show that f' is surjective, so choose a short exact sequence

$$0 \to G_0 \to E_0 \to \mathbb{Q} \to 0$$

representing a class $\xi_0 \in \mathrm{Ext}^1_{R_0}(\mathbb{Q}, G_0)$. The vanishing of $\mathrm{H}^1(S_0, G_0)$ for all finite R_0-algebras S_0 implies that we obtain a short exact sequence on S_0-points for any S_0, and constant Zariski sheaves on $\mathscr{C}_R$ are sheaves for the finite flat topology, so pushforward along $j : \mathrm{Spec}(R_0) \to \mathrm{Spec}(R)$ gives an exact sequence

$$0 \to j_*(G_0) \to j_*(E_0) \to \mathbb{Q} \to 0.$$

Since $\mathfrak{m}J = 0$ and G is formally smooth, we have a short exact sequence

$$0 \to \mathscr{K} \to G \to j_*(G_0) \to 0$$

on $\mathscr{C}_R$ where $\mathscr{K}(S) = \mathrm{Lie}(G_\kappa) \otimes_\kappa JS$ for any finite R-algebra S. Thus, $p : G \to G$ factors uniquely through a map $h : j_*(G_0) \to G$ since $p\mathcal{K} = 0$, and the pushout of $j_*(E_0)$ along h is an extension of $\mathbb{Q}$ by G whose pullback over R_0 is $p\xi_0$. Since p acts invertibly on $\mathbb{Q}$, we conclude that f' is surjective. $\square$

We have settled the formal smoothness in Theorem 1.4.4.7. Before we address the other assertions, we make a practical observation:

1.4.4.10. Remark. The infinitesimal liftability of p-divisible groups, Zariski locally on the base, is a hypothesis which underlies the Grothendieck–Messing crystalline Dieudonné theory [**75**, Ch. IV, V] that classifies the deformations of p-divisible groups. It is a deep theorem of Grothendieck–Illusie that this liftability property holds without Zariski-localization over any affine base on which p is nilpotent (see [**51**, 4.4]). To apply Grothendieck–Messing theory over artinian local base rings (which is all we really need in this book) it suffices to use the formal smoothness established above.

Continuing with the proof of Theorem 1.4.4.7, we address Schlessinger's criteria for pro-representability of $F = \mathrm{Def}_\Lambda(X_0)$ (and compute its tangent space). Consider a pair of maps $R_1, R_2 \rightrightarrows R_0$ in $\mathcal{C}_\Lambda$ with $R_1 \to R_0$ surjective. Since deformations of p-divisible groups over artinian local rings have no non-trivial automorphisms, the bijectivity of

$$F(R_1 \times_{R_0} R_2) \to F(R_1) \times_{F(R_0)} F(R_2)$$

is immediate from part (2) of the following general result (which will be very useful in our later work with algebraization of formal CM abelian schemes; see Theorem 2.2.3).

1.4.4.11. Proposition (Ferrand)**.** *Let $p_1 : R_1 \to R_0$ and $p_2 : R_2 \to R_0$ be maps of rings with p_1 surjective. Let R denote the fiber product ring $R_1 \times_{R_0} R_2$.*

(1) *If M is a flat R-module and M_j denotes the flat R_j-module $M \otimes_R R_j$ then the natural map $M \to M_1 \times_{M_0} M_2$ is an isomorphism. Conversely, if M_j is an R_j-module and there are given isomorphisms $R_0 \otimes_{R_1} M_1 \simeq M_0 \simeq R_0 \otimes_{R_2} M_2$ then for the R-module $M = M_1 \times_{M_0} M_2$ the natural maps $R_j \otimes_R M \to M_j$ are isomorphisms, and M is R-flat when each M_j is R_j-flat.*

(2) *Let R'_j be a finitely generated R_j-algebra and suppose there are given isomorphisms of R_0-algebras $R_0 \otimes_{R_1} R'_1 \simeq R'_0 \simeq R_0 \otimes_{R_2} R'_2$. The R-algebra $R' := R'_1 \times_{R'_0} R'_2$ is finitely generated, and if each R'_j is flat and finitely presented over R_j then R' is flat and finitely presented over R.*

(3) *Assume that p_2 is surjective or that all elements of $\ker(p_1)$ are nilpotent. The functor*

$$X \rightsquigarrow (X_{R_1}, X_{R_2}, (X_{R_1})_{R_0} \simeq (X_{R_2})_{R_0})$$

from the category of flat R-schemes to the category of triples (X_1, X_2, f) consisting of flat schemes X_j over R_j and an R_0-isomorphism $f : (X_1)_{R_0} \simeq (X_2)_{R_0}$ is an equivalence, and X is finite type (respectively flat and finitely presented) over R if and only if each X_j is finite type (respectively flat and finitely presented) over R_j.

An R-map $f : X \to Y$ between flat finitely presented R-schemes satisfies property $\mathbf{P}$ if and only if the pullback maps f_{R_1} and f_{R_2} satisfy $\mathbf{P}$, where $\mathbf{P}$ is any of the properties: separated, proper, finite, flat, smooth, étale, isomorphism, geometric fibers of pure dimension d, connected geometric fibers.

Generalizations of parts (2) and (3) are given in [**101**, Appendix A] (and references therein). For applications to Schlessinger's criteria, part (3) is used with

$\ker(p_1)$ nilpotent. In other situations (such as gluing along closed subschemes, which we need in the proof of Theorem 2.2.3) part (3) is used with surjective p_2.

PROOF. Part (1) is [**40**, Thm. 2.2(iv)] (upon noting that by the *proof* of [**40**, Thm. 2.2(iii)], the kernel vanishes when M is R-flat). We prove part (2) by using a limit argument suggested by D. Rydh. First assume that each R'_j is finitely generated over R_j. Consider the directed system $\{R'_\alpha\}$ of finitely generated R-subalgebras of R', and let $R'_{j,\alpha} = R'_\alpha \otimes_R R_j$, so $\varinjlim R'_{j,\alpha} = R'_j$ for each j (since $R' \otimes_R R_j \to R'_j$ is an isomorphism by part (1) applied to $M = R'$). Since each R'_j is finitely generated over R_j, it follows that for sufficiently large α_0 the maps $R'_{j,\alpha_0} \to R'_j$ are surjective for all j. In other words, for the cokernel R-module $M = \operatorname{coker}(R'_{\alpha_0} \to R')$, both $M \otimes_R R_1$ and $M \otimes_R R_2$ vanish. Hence, $M = 0$ by [**40**, Thm. 2.2(ii)]. This says that the inclusion $R'_{\alpha_0} \subset R'$ is an equality, so R' is finitely generated over R.

Now assume that each R'_j is flat and finitely presented over R_j, so R' is flat and finitely generated over R. Form a presentation

$$0 \to I \to R[t_1, \dots, t_n] \to R' \to 0.$$

By the R-flatness of R', I is R-flat and this sequence remains exact after applying $R_j \otimes_R (\cdot)$. Thus, the finite presentation of R'_j over R_j implies that the ideal $I_j = R_j \otimes_R I$ is finitely generated as a module over $P_j = R_j[t_1, \dots, t_n]$ for each j. By part (1) applied to the R-flat I, we have $I = I_1 \times_{I_0} I_2$. Letting $P = R[t_1, \dots, t_n]$, clearly $P = P_1 \times_{P_0} P_2$ for surjections $P_1, P_2 \rightrightarrows P_0$, and $I_j = P_j \otimes_P I$. Since $I = I_1 \times_{I_0} I_2$, a variation on the limit argument in the proof of (2) (now applied to modules over R rather than algebras over R) shows that the P-module $I = I_1 \times_{I_0} I_2$ is finitely generated since each I_j is finitely generated over P_j.

To prove (3), first we prove the equivalences of categories. Assume p_2 is surjective. The key point in this case is that for closed immersions of schemes $Z \hookrightarrow Y$ and $Z \hookrightarrow Y'$ the associated pushout of ringed spaces $Y \coprod_Z Y'$ (topological space gluing and fiber product of structure sheaves) is again a scheme, identified in the evident manner with the spectrum of a ring-theoretic fiber product when Y, Y', and Z are affine. The proof of this assertion is elementary and left to the reader; it is made easier by first showing that the ringed space gluing has the expected universal property among ringed spaces and is compatible with topological localization, and then proving it is isomorphic in the expected way to the desired affine scheme when Y, Y', and Z are affine. (See [**21**, §2] for further discussion of this argument, and [**40**, §7], [**62**, Thm. 38], [**81**, §3], [**101**, Appendix A] for more general existence results for pushouts.)

By part (1), the formation of the pushout $Y \coprod_Z Y'$ is compatible with flat base change over the pushout, so if X is a flat R-scheme then it is the pushout of its closed subschemes X_{R_1} and X_{R_2} along their common closed subscheme $X_{R_0} = (X_{R_1})_{R_0} = (X_{R_2})_{R_0}$. The equivalence of categories in (3) therefore follows from (1) and the existence of the general "gluing" of schemes along a closed subscheme and its compatibility with Zariski-localization (so we may carry out computations in the affine setting).

Suppose instead that the elements of $\ker(p_1)$ are nilpotent. Now the relevant pushout we must construct is relative to a closed immersion of schemes $j : Z \hookrightarrow Y$ that is topologically an equality (i.e., all sections of the defining quasi-coherent ideal sheaf are locally nilpotent) and an affine map $f' : Z \to Y'$. For every affine open

$U' \subset Y'$, the preimage affine open ${f'}^{-1}(U')$ in Z underlies an open subscheme of Y that is also affine (since affineness is determined by the underlying reduced scheme [**24**, A.2]). We define the pushout ringed space $Y \coprod_Z Y'$ to have the same topological space as Y' and structure sheaf $f'_*(\mathcal{O}_Y) \times_{f'_*(\mathcal{O}_Z)} \mathcal{O}_{Y'}$ (via the identification of $\mathcal{O}_Y$ as a sheaf on the topological space of Z). By working Zariski-locally on Y' this is easily checked to be a scheme, coinciding in the evident manner with the spectrum of the expected fiber product ring when Y', Y, and Z are affine. Thus, the equivalence of categories in (3) follows via (1) as in the case when p_2 is surjective.

Finally, we analyze the behavior of various properties $\mathbf{P}$ of R-scheme morphisms $h : X \to Y$ between two flat R-schemes of finite presentation when either p_2 is surjective or $\ker(p_1)$ consists of nilpotent elements. Let $Y_j = Y_{R_j}$ and $X_j = X_{R_j}$. Note that if $\ker(p_1)$ consists of nilpotent elements then the map $\mathrm{Spec}(R) \to \mathrm{Spec}(R_2)$ is a closed immersion defined by an ideal of nilpotent elements, so the same holds for $X \to X_2$ and $Y \to Y_2$. The two cases (surjective p_2, or $\ker(p_1)$ consisting of nilpotent elements) now will be treated simultaneously.

Clearly the map induced by h between fibers over a point in $\mathrm{Spec}(R)$ is identified with the analogous fiber map for the one of the pullbacks $h_j : X_j \to Y_j$ over R_j with $j \in \{1, 2\}$. Hence, since X and Y are R-flat of finite presentation, the fibral flatness criterion [**34**, IV_3, 11.3.11] implies that h is flat if and only if h_1 and h_2 are flat. By the fibral smoothness, étaleness, and isomorphism criteria [**34**, IV_4, 17.8.2, 17.9.5], the cases when $\mathbf{P}$ is "smooth", "étale", or "isomorphism" are also settled. The cases of geometric fibers being connected or of pure dimension d are obvious.

Since h is finite if and only if it is quasi-finite and proper [**34**, IV_3, 8.11.1], and the finite type h is quasi-finite if and only if h_1 and h_2 are quasi-finite, the case when $\mathbf{P}$ is "finite" is reduced the case when $\mathbf{P}$ is "proper". When h_1 and h_2 are universally closed it is clear that h is universally closed, so it remains to treat the case of separatedness; i.e., closedness of the diagonal $\Delta_{X/Y}$. Topologically this map is visibly a gluing of Δ_{X_1/Y_1} and Δ_{X_2/Y_2} when p_2 is surjective, and it coincides topologically with Δ_{X_2/Y_2} when $\ker(p_1)$ consists of nilpotent elements. Thus, in both cases separatedness of h_1 and h_2 implies separatedness of h. □

We have established enough compatibility for $F = \mathrm{Def}_\Lambda(X_0)$ with respect to fiber products in $\mathcal{C}_\Lambda$ to equip the tangent space t_{X_0} with a natural κ-vector space structure. Thus, to complete the verification of Schlessinger's criteria we need to address the finite-dimensionality of t_{X_0}.

Equip the square-zero kernel of $\kappa[\epsilon] \twoheadrightarrow \kappa$ with trivial divided powers, so by Grothendieck–Messing theory [**75**, Ch. IV, V] we can classify the deformations X of X_0 over $\kappa[\epsilon]$ in terms of the subbundle $\mathrm{Lie}(X^t)^\vee$ of the Lie algebra of the universal vector extension $\mathrm{E}(X)$ of X; here, $\mathrm{E}(X)$ is universal among extensions of X by the vector group $\mathrm{Lie}(X^t)^\vee$. (This application of Grothendieck–Messing theory does not rest on the caveats as in Remark 1.4.4.10 since $\kappa \to \kappa[\epsilon]$ has a section.) Via the choice of divided powers, the Lie algebra $\mathrm{Lie}(\mathrm{E}(X))$ is *canonically* isomorphic to the Lie algebra

$$\mathrm{Lie}(\mathrm{E}((X_0)_{\kappa[\epsilon]})) = \mathrm{Lie}(\mathrm{E}(X_0)) \otimes_\kappa \kappa[\epsilon]$$

associated to the constant deformation (the "origin" of the tangent space), and there are canonical exact sequences

$$0 \to \mathrm{Lie}(X^t)^\vee \to \mathrm{Lie}(\mathrm{E}(X)) \to \mathrm{Lie}(X) \to 0$$

over $\kappa[\epsilon]$ and

$$0 \to \mathrm{Lie}(X_0^t)^\vee \to \mathrm{Lie}(\mathrm{E}(X_0)) \to \mathrm{Lie}(X_0) \to 0$$

over κ.

Grothendieck–Messing theory identifies t_{X_0} with the set of $\kappa[\epsilon]$-subbundles of $\mathrm{Lie}(\mathrm{E}(X_0)) \otimes_\kappa \kappa[\epsilon]$ which lift $\mathrm{Lie}(X_0^t)^\vee$ modulo ϵ. Such subbundles are parameterized by

$$\begin{aligned} \mathrm{Hom}(\mathrm{Lie}(X_0^t)^\vee, \mathrm{Lie}(\mathrm{E}(X_0)))/\operatorname{End}(\mathrm{Lie}(X_0^t)^\vee) &= \mathrm{Hom}(\mathrm{Lie}(X_0^t)^\vee, \mathrm{Lie}(X_0)) \\ &= \mathrm{Lie}(X_0^t) \otimes_\kappa \mathrm{Lie}(X_0) \end{aligned}$$

by assigning to any representative κ-linear map $L : \mathrm{Lie}(X_0^t)^\vee \to \mathrm{Lie}(\mathrm{E}(X_0))$ the $\kappa[\epsilon]$-subbundle that is the image of the map $\mathrm{Lie}(X_0^t)^\vee \otimes_\kappa \kappa[\epsilon] \to \mathrm{Lie}(\mathrm{E}(X_0)) \otimes_\kappa \kappa[\epsilon]$ defined by $x + y\epsilon \mapsto x + (y + L(x))\epsilon$. Our computation of t_{X_0} respects the κ-linear structure on t_{X_0}, so this completes the proof of Theorem 1.4.4.7. ☐

As an extension of Theorem 1.4.4.7, in Theorem 1.4.5.5 we will establish a "p-divisible group" version of the second part of Theorem 1.4.4.5. We finish the present discussion of deformation theory by addressing the useful topic of how deformation rings behave with respect to "change of coefficients". This is relevant when trying to reduce certain structural questions about deformation rings (e.g., is there a characteristic-0 point?) to the case of an algebraically closed residue field.

1.4.4.12. Example. Consider a local map $\Lambda \to \Lambda'$ between complete local noetherian rings with respective residue fields κ and κ', and let X be a proper κ-scheme such that any proper flat deformations of X over artin local Λ-algebras with residue field κ admit no non-trivial automorphisms, and similarly for $X_{\kappa'}$ using Λ'-algebras. The deformation functor $\mathrm{Def}_\Lambda(X)$ assigns to any artin local Λ-algebra R with residue field κ the set of isomorphism classes of proper flat deformations of X over R, and we define $\mathrm{Def}_{\Lambda'}(X_{\kappa'})$ similarly.

It is a theorem of Schlessinger that $\mathrm{Def}_\Lambda(X)$ is pro-represented by a complete local noetherian Λ-algebra $\mathcal{R}$ with residue field κ, and likewise $\mathrm{Def}_{\Lambda'}(X_{\kappa'})$ is pro-represented by a complete local noetherian Λ'-algebra $\mathcal{R}'$ with residue field κ'. Note that $\Lambda'\widehat{\otimes}_\Lambda\mathcal{R}$ is a complete local noetherian Λ'-algebra with residue field κ'. By the local flatness criterion [**73**, 22.4], base change along $\mathcal{R} \to \Lambda'\widehat{\otimes}_\Lambda\mathcal{R}$ carries flat formal $\mathcal{R}$-schemes of finite type to flat formal $\Lambda'\widehat{\otimes}_\Lambda\mathcal{R}$-schemes of finite type.

Let $\mathfrak{X}$ and $\mathfrak{X}'$ be the universal formal deformations of X and $X_{\kappa'}$ over $\mathcal{R}$ and $\mathcal{R}'$ respectively. Clearly

$$\mathfrak{X} \times_{\mathrm{Spf}(\mathcal{R})} \mathrm{Spf}(\Lambda'\widehat{\otimes}_\Lambda\mathcal{R}) \to \mathrm{Spf}(\Lambda'\widehat{\otimes}_\Lambda\mathcal{R})$$

is a proper flat deformation of $X_{\kappa'}$, so it arises as the pullback of $\mathfrak{X}'$ along a unique local Λ'-algebra map

$$\mathcal{R}' \to \Lambda'\widehat{\otimes}_\Lambda\mathcal{R}. \tag{1.4.4.2}$$

Is this map an isomorphism?

To demonstrate the usefulness of an affirmative answer, suppose κ and κ' are perfect of characteristic $p > 0$, and $\Lambda = W(\kappa)$ and $\Lambda' = W(\kappa')$. (The case $\kappa' = \overline{\kappa}$ will be of most interest.) Consider the problem of whether or not X admits a proper flat formal lift over a complete local noetherian domain with residue field κ and characteristic 0. Suppose we can establish that $X_{\kappa'}$ admits a proper flat formal lift over a complete local noetherian domain D' with residue field κ' and characteristic 0. This lift corresponds to a local $W(\kappa')$-algebra homomorphism

$\mathcal{R}' \to D'$, so if (1.4.4.2) is an isomorphism then we obtain a local $W(\kappa)$-algebra homomorphism $\mathcal{R} \to D'$. Hence, $\mathcal{R}[1/p] \neq 0$, so by [**54**, 7.1.9] (which interprets the closed points of $\mathrm{Spec}(\mathcal{R}[1/p])$ in terms of rigid-analytic geometry) there is a local $W(\kappa)$-homomorphism from $\mathcal{R}$ into the valuation ring of a field F of finite degree over $W(\kappa)[1/p]$. The image of $\mathcal{R}$ in $\mathcal{O}_F$ is a (possibly non-normal) local domain that is finite flat over $W(\kappa)$ and has residue field κ. (See 2.1.1 for another instance of this slicing argument in deformation rings.)

To summarize, if (1.4.4.2) is an isomorphism then the problem of finding a formal lift of X to characteristic 0 with residue field κ is reduced to the same problem for $X_{\kappa'}$ with residue field κ'. In other words, the formal flat lifting problem with a *fixed* residue field is unaffected by making a preliminary scalar extension to κ'! This is useful when $\kappa' = \overline{\kappa}$ because it is often easier to make constructions without increasing the residue field when the residue field is algebraically closed.

The problem of compatibility of the deformation ring with respect to change of the coefficients (i.e., the isomorphism problem for analogues of (1.4.4.2)) arises in applications ranging from moduli problems in algebraic geometry to Galois deformation theory and beyond. In the special case that Λ' is the finite étale extension of Λ corresponding to a finite separable extension κ' of κ, an affirmative answer to the isomorphism problem for the pair (Λ, Λ') can be established within the axiomatic deformation theory framework presented by Rim in [**100**, 1.15–1.19], which considers more general Λ' for which κ' is just finitely generated over κ. However, to include the case $\kappa' = \overline{\kappa}$ all finiteness hypotheses on κ'/κ must be avoided. There is an axiomatic approach to the "change of coefficients" problem (in the spirit of Schlessinger's criteria), independent of the methods of SGA7, but for the present purposes it is simpler to give direct proofs in the cases we need. Later we will need the abstract criterion, at which point we will state and prove it. (See Proposition 1.4.5.6.)

For the formal deformation rings of abelian varieties and p-divisible groups (without extra structure), the isomorphism property for the analogue of (1.4.4.2) is easy to verify:

1.4.4.13. Proposition. *Let $\Lambda \to \Lambda'$ be a local map between complete local noetherian rings, inducing an extension $\kappa \to \kappa'$ of residue fields. Let G_0 be an abelian variety or p-divisible group over κ, and $G_0' = (G_0)_{\kappa'}$. In the case of p-divisible groups, assume* $\mathrm{char}(\kappa) = p$.

For the deformation rings $\mathcal{R}$ and $\mathcal{R}'$ pro-representing $\mathrm{Def}_\Lambda(G_0)$ *and* $\mathrm{Def}_{\Lambda'}(G_0')$ *respectively, the natural map*

$$\mathcal{R}' \to \Lambda' \widehat{\otimes}_\Lambda \mathcal{R}$$

is an isomorphism.

PROOF. In both cases, the map in question is between formal power series rings over Λ'. Hence, it suffices to check that the induced map between relative tangent spaces over κ' is an isomorphism. In each case, the tangent map is identified with the natural map

$$\kappa' \otimes_\kappa (\mathrm{Lie}(G_0^t) \otimes_\kappa \mathrm{Lie}(G_0)) \to \mathrm{Lie}((G_0')^t) \otimes_{\kappa'} \mathrm{Lie}(G_0') \tag{1.4.4.3}$$

that is an isomorphism. Indeed, in the case of abelian varieties this compatibility follows from the functoriality in the ground field for the general identification of the tangent space of the deformation functor of a proper κ-scheme Y_0 with $\mathrm{H}^1(Y_0, (\Omega^1_{Y_0/\kappa})^\vee)$. In the case of p-divisible groups it follows from the compatibility of Grothendieck–Messing theory with respect to base change. □

Deformation rings for geometric objects equipped with extra structure (e.g., polarized abelian varieties with endomorphism structure) are not as easy to describe as in the formally smooth setting used in the preceding proof. In such cases we can sometimes use a global moduli scheme to establish an isomorphism result for the "change of coefficients" map:

1.4.4.14. Proposition. *Let Λ be a complete local noetherian ring with residue field κ, and let (A_0, ϕ_0, α_0) be a polarized abelian variety of dimension $g > 0$ with endomorphism structure $\alpha_0 : \mathcal{O} \hookrightarrow \mathrm{End}(A_0)$ for a $\mathbb{Z}$-finite associative ring $\mathcal{O}$. The analogue of* (1.4.4.2) *for (A_0, ϕ_0, α_0) is an isomorphism for any Λ'.*

The same "change of coefficients" isomorphism holds for the formal deformation ring of any pair (A_0, α_0).

Proof. First we treat the polarized cases by relating the deformation problem to global moduli schemes via auxiliary "level structure", and then we modify the method to apply in the absence of polarizations. The introduction of auxiliary level structure can be carried out without increasing κ by using non-constant "finite étale level structure" arising inside A_0, as follows.

Fix an integer $n \geqslant 3$ not divisible by $\mathrm{char}(\kappa)$. The finite étale group scheme $A_0[n]$ over κ uniquely lifts to a finite étale group scheme $\mathcal{G}$ over Λ. Consider the functor F on the category of Λ-schemes that assigns to any Λ-scheme S the set of isomorphism classes of quadruples (A, ϕ, α, τ) where (A, ϕ) is a polarized abelian scheme over S of relative dimension g with ϕ of constant square degree $\deg(\phi_0)$, $\alpha : \mathcal{O} \to \mathrm{End}(A)$ is a homomorphism, and $\tau : A[n] \simeq \mathcal{G}_S$ is an S-group isomorphism ("level structure"). These quadruples have no nontrivial automorphisms since $n \geqslant 3$ and $n \in \Lambda^\times$.

By standard moduli space arguments (using Hilbert schemes), the functor F is represented by a Λ-scheme $\mathcal{M}$ locally of finite type. The triple (A_0, ϕ_0, α_0) and the canonical isomorphism $\tau_0 : \mathcal{G}_\kappa \simeq A_0[n]$ define a point $\xi \in \mathcal{M}(\kappa)$, and the formal deformation ring for (A_0, ϕ_0, α_0) is naturally isomorphic to the completed local ring $\mathcal{O}^\wedge_{\mathcal{M},\xi}$ at ξ (since the finite étale "level structure" τ_0 uniquely lifts through any infinitesimal deformation).

Since $\mathcal{M}_{\Lambda'}$ represents the restriction of F to the category of Λ'-schemes, it is straightforward to verify that the analogue of (1.4.4.2) for the present situation is the inverse of the natural isomorphism

$$\Lambda' \widehat{\otimes}_\Lambda \mathcal{O}^\wedge_{\mathcal{M},\xi} \simeq \mathcal{O}^\wedge_{\mathcal{M}_{\Lambda'},\xi_{\kappa'}},$$

so it is an isomorphism. (This style of argument applies whenever we can relate the infinitesimal deformation problem to the formal structure on a global moduli scheme over Λ.)

Now we treat the case of formal deformation rings for (A_0, α_0) and (A'_0, α'_0) relative to some $\Lambda \to \Lambda'$. The absence of a polarization eliminates the option to use global moduli schemes for abelian schemes. Instead, we work with formal Hom-schemes attached to formal abelian schemes. (The same procedure can be used to handle the polarized case above.) Let $\mathfrak{A} \to \mathrm{Spf}(\mathcal{R})$ be the universal deformation of A_0, so for $\mathcal{R}' := \Lambda'\widehat{\otimes}_\Lambda \mathcal{R}$ it follows from Proposition 1.4.4.13 that the universal deformation of A'_0 is the base change

$$\mathfrak{A}' = \mathfrak{A} \times_{\mathrm{Spf}(\mathcal{R})} \mathrm{Spf}(\mathcal{R}') \to \mathrm{Spf}(\mathcal{R}').$$

For any formal abelian schemes $\mathfrak{B}$ and $\mathfrak{C}$ over a complete local noetherian ring R, applying the arguments with Hom-functors from the proof of Theorem 1.4.4.5 over the artinian quotients of R proves that the Hom-functor $\underline{\mathrm{Hom}}(\mathfrak{B}, \mathfrak{C}) : \mathfrak{Y} \rightsquigarrow \mathrm{Hom}_{\mathfrak{Y}\text{-gp}}(\mathfrak{B}_{\mathfrak{Y}}, \mathfrak{C}_{\mathfrak{Y}})$ on the category of formal (adic) R-schemes $\mathfrak{Y}$ locally of finite type is represented by a separated and locally finite type formal R-scheme.

Thus, we get a separated and locally finite type formal $\mathcal{R}$-scheme $\underline{\mathrm{End}}(\mathfrak{A})$ classifying endomorphisms of $\mathfrak{A}$, and its formation commutes with local base change to any complete local noetherian ring (such as $\mathcal{R}'$). The definition of an action on (a base change of) $\mathfrak{A}$ by the $\mathbb{Z}$-finite ring $\mathcal{O}$ underlying α_0 amounts to giving several points of $\underline{\mathrm{End}}(\mathfrak{A})$ satisfying finitely many relations. These relations correspond to a formal closed subscheme in a fiber power of $\mathrm{End}(\mathfrak{A})$, so we get an adic formal moduli scheme $\mathfrak{M}$ locally of finite type over $\mathcal{R}$ that classifies $\mathcal{O}$-actions on $\mathfrak{A}$. Moreover, the formation of $\mathfrak{M}$ commutes with base change along any local homomorphism from $\mathcal{R}$ to another complete local noetherian ring.

The given α_0 corresponds to a rational point $\xi \in \mathfrak{M}(\kappa)$ in the special fiber, and the deformation ring pro-representing $\mathrm{Def}_\Lambda(A_0, \alpha_0)$ is the completed local ring $\mathcal{O}^\wedge_{\mathfrak{M},\xi}$. Similarly, $\mathfrak{M}' := \mathfrak{M}_{\mathcal{R}'}$ contains the κ'-point ξ' in its special fiber that corresponds to α'_0 and arises by base change from ξ, so there is a natural isomorphism

$$\Lambda'\widehat{\otimes}_\Lambda \mathcal{O}^\wedge_{\mathfrak{M},\xi} \simeq \mathcal{O}^\wedge_{\mathfrak{M}',\xi'}.$$

The inverse of this isomorphism is the "change of coefficients" map that we wanted to prove is an isomorphism. □

1.4.5. Hodge–Tate decomposition and Serre–Tate lifts. We finish our summary of the theory of p-divisible groups by recording (for later reference) two fundamental theorems. The first is a deep result of Tate.

1.4.5.1. Theorem (Tate)**.** *Let R be a complete discrete valuation ring with perfect residue field of characteristic $p > 0$ and fraction field K of characteristic* 0*. For any p-divisible groups G and G' over R, the natural injective map* $\mathrm{Hom}(G, G') \to \mathrm{Hom}(G_K, G'_K)$ *is bijective. Moreover, if $\mathbb{C}_K$ denotes the completion of an algebraic closure $\overline{K}$ of K then there is a canonical $\mathbb{C}_K$-linear $\mathrm{Gal}(\overline{K}/K)$-equivariant isomorphism*

$$\mathbb{C}_K \otimes_{\mathbb{Q}_p} V_p(G_{\overline{K}}) \simeq (\mathbb{C}_K(1) \otimes_K \mathrm{Lie}(G)_K) \oplus (\mathbb{C}_K \otimes_K \mathrm{Lie}(G^t)^\vee_K). \tag{1.4.5.1}$$

Proof. The full faithfulness of $G \rightsquigarrow G_K$ is [**119**, 4.2], and the construction of the isomorphism (1.4.5.1) occupies most of [**119**]. □

A useful application of the full faithfulness in Tate's theorem is "completed unramified descent" for p-divisible groups:

1.4.5.2. Corollary. *Let R be as in Theorem* 1.4.5.1 *and let K' be the completion of the maximal unramified extension of K inside $\overline{K}$. Let G' be a p-divisible group over the valuation ring R' of K', and assume that the generic fiber $G'_{K'}$ is equipped with a descent to a p-divisible group X over K.*

There is a pair (G, α) consisting of a p-divisible group G over R and an isomorphism $\alpha : G_K \simeq X$ over K. Moreover, there is a unique isomorphism $G_{R'} \simeq G'$ recovering the given identification of generic fibers $X \otimes_K K' \simeq G' \otimes_{R'} K'$.

A special case of this corollary is that any "unramified twist" of the p-adic Tate module of the generic fiber of a p-divisible group over R is also the p-adic Tate module of the generic fiber of a p-divisible group over R (since both p-adic Galois lattices have the same inertial restriction).

PROOF. The discrete valuation ring R' is the completion of the strict henselization R^{sh} of R inside $\overline{K}$, so $R^{\mathrm{sh}} \to R'$ is a local inclusion with relative ramification degree 1 and induces an isomorphism on residue fields. Thus, for any affine R'-scheme Y', descent of $Y'_{K'}$ to $K^{\mathrm{sh}} = \mathrm{Frac}(R^{\mathrm{sh}})$ is equivalent to descent of Y' to R^{sh} [**10**, 6.2, Prop. D.4]. Applying this to each $G'[p^n]$, we see that G' uniquely descends to a p-divisible group $\mathscr{G}$ over R^{sh} compatibly with the descent $X_{K^{\mathrm{sh}}}$ of $G'_{K'}$.

For each $\sigma \in \mathrm{Gal}(K^{\mathrm{sh}}/K)$ and the associated continuous K-automorphism σ' of the completion K', the canonical isomorphism $\sigma^*(X_{K^{\mathrm{sh}}}) \simeq X_{K^{\mathrm{sh}}}$ induces an isomorphism $\sigma'^*(G'_{K'}) \simeq G'_{K'}$. By Tate's full faithfulness result (applied over R'), this extends to an isomorphism $\sigma'^*(G') \simeq G'$ of p-divisible groups over R'. The uniqueness of the descent from R' to R^{sh} implies that this latter isomorphism uniquely descends to an R^{sh}-isomorphism $\alpha_\sigma : \sigma^*(\mathscr{G}) \simeq \mathscr{G}$ extending the canonical isomorphism $\sigma^*(X_{K^{\mathrm{sh}}}) \simeq X_{K^{\mathrm{sh}}}$.

The 1-cocycle condition $\alpha_\tau \circ \tau^*(\alpha_\sigma) = \alpha_{\tau\sigma}$ over R^{sh} is inherited from the generic fiber. Thus, since R^{sh} is a direct limit of R-subalgebras that are Galois local finite étale over R, on each *finite* p^n-torsion level the R^{sh}-isomorphisms α_σ amount to an étale descent datum relative to $R \to R^{\mathrm{sh}}$ [**10**, 6.2/B]. The resulting effective descent of $\mathscr{G}$ to a p-divisible group G over R is equipped with a canonical K-isomorphism $\alpha : G_K \simeq X$. By Tate's full faithfulness theorem applied over R', the K'-isomorphism

$$(G_{R'}) \otimes_{R'} K' = G_K \otimes_K K' \simeq X_{K'} \simeq G' \otimes_{R'} K'$$

uniquely extends to an R'-isomorphism $G_{R'} \simeq G'$. □

The link between the deformation theories of abelian varieties and p-divisible groups in characteristic p is provided by the Serre-Tate deformation theorem:

1.4.5.3. Theorem (Serre–Tate). *Let R be a ring in which a prime p is nilpotent, and let I be an ideal in R such that $I^n = 0$ for some $n \geqslant 1$. Define $R_0 = R/I$, and for an abelian scheme A and p-divisible group G over R let A_0 and G_0 denote their respective reductions modulo I.*

For any abelian scheme A over R, let $\epsilon_A : A[p^\infty]_0 \simeq A_0[p^\infty]$ denote the canonical isomorphism. The functor $A \rightsquigarrow (A_0, A[p^\infty], \epsilon_A)$ from the category of abelian schemes over R to the category of triples $(A_0, G, \epsilon : A[p^\infty]_0 \simeq G_0)$ is an equivalence.

See [**57**, 1.2.1] for a proof of this result. □

The most important application of the Serre-Tate deformation theorem is that for an abelian variety A_0 over a field of characteristic $p > 0$, the infinitesimal deformation theory of A_0 coincides with that of its p-divisible group. Likewise, if we fix a subring $\mathcal{O} \subset \mathrm{End}(A_0)$ or a polarization of A_0 (or both) then via the injection $\mathrm{End}(A_0) \subset \mathrm{End}(A_0[p^\infty])$ (Proposition 1.2.5.1) and the identification of

$A_0^t[p^\infty]$ with the Cartier dual of $A_0[p^\infty]$, the infinitesimal deformation theory of A_0 equipped with this extra structure is the same as that of its p-divisible group equipped with the analogous induced extra structure.

Consider a homomorphism $\phi_0 : A_0 \to A_0^t$ and the associated homomorphism

$$f_0 : A_0[p^\infty] \to A_0^t[p^\infty] \simeq A_0[p^\infty]^t.$$

Clearly ϕ_0 is an isogeny if and only if f_0 is an isogeny, and we saw in 1.4.3.4 that ϕ_0 is symmetric with respect to double duality of abelian varieties if and only if f_0 is skew-symmetric (i.e., $f_0^t = -f_0$) with respect to the canonical isomorphism of a p-divisible group with its Serre double dual.

This leads us to define a *quasi-polarization* of a p-divisible group G over a complete local noetherian ring to be a skew-symmetric homomorphism $f : G \to G^t$ that induces an isogeny between the special fibers. (We will see in 3.3.8 that it is equivalent to say the skew-symmetric f is an isogeny in the sense of 3.3.5, so we can thereby define the notion of quasi-polarization over any base scheme.) The ampleness aspect of a polarization cannot be encoded in terms of p-divisible groups, but quasi-polarizations are nonetheless a helpful concept when using p-divisible groups to study abelian varieties and their deformations, as the following example illustrates.

1.4.5.4. Example. As a special case of the Serre-Tate deformation theorem, if R is a complete local noetherian ring of residue characteristic $p > 0$ and A_0 is an abelian variety over the residue field, then a deformation of $A_0[p^\infty]$ to a p-divisible group G over R corresponds to a deformation of A_0 to a formal abelian scheme $\mathfrak{A}$ over R. If A_0 is equipped with a CM structure and we demand that this structure lifts to $\mathfrak{A}$ (via the injection $\mathrm{End}(\mathfrak{A}) \hookrightarrow \mathrm{End}(A_0)$) then $\mathfrak{A}$ can fail to be algebraic (i.e., it may not be the formal completion of a proper R-scheme). Explicit CM examples of this type are given in 4.1.2; also see the discussion immediately following the statement of Theorem 2.2.3.

To ensure algebraicity of $\mathfrak{A}$, we need to encode the deformation of a polarization. More specifically, choose a polarization $\phi_0 : A_0 \to A_0^t$ and suppose that the corresponding map $f : A_0[p^\infty] \to A_0^t[p^\infty] = A_0[p^\infty]^t$ lifts to R (as can happen in at most one way, by Proposition 1.4.4.3). Let $\phi : \mathfrak{A} \to \mathfrak{A}^t$ be the corresponding unique homomorphism that lifts ϕ_0 (in accordance with the Serre–Tate deformation theorem). If $\mathfrak{P}$ denotes the formal Poincaré bundle on $\mathfrak{A} \times \mathfrak{A}^t$ (which lifts the Poincaré bundle $\mathscr{P}_0$ on $A_0 \times A_0^t$) then $(1, \phi)^*\mathfrak{P}$ is a line bundle on $\mathfrak{A}$ lifting the line bundle $(1, \phi_0)^*\mathscr{P}_0$ on A_0 that is ample (due to ϕ_0 being a polarization). Hence, by Grothendieck's algebraization theorems [**34**, III_1, 5.4.1, 5.4.5], in such cases $\mathfrak{A}$ is algebraic, so it arises from a unique abelian R-scheme A deforming A_0.

There is a special case in which the liftability of all polarizations comes "for free": the *Serre–Tate canonical lifting* of an *ordinary* abelian variety A_0 over a perfect field k of characteristic $p > 0$. To explain these concepts, we first note that by the perfectness of k, the connected-étale sequence of every p-divisible group X over k is split (exactly as for finite commutative k-groups), so X is (uniquely) the product of an étale p-divisible group and a connected p-divisible group; see [**87**, I.2]. Letting $g = \dim(A_0)$, since an étale p-divisible group over k has connected Serre dual (as we may check over $\overline{k}$) and $A_0[p^\infty] = A_0[p^\infty]^0 \times A_0[p^\infty]^{\text{ét}}$ is of height $2g$ yet isogenous to its Serre dual $A_0[p^\infty]^t \simeq A_0^t[p^\infty]$ (as A_0 is isogenous to A_0^t), we see that the *p-rank* of $A_0[p^\infty]$ (i.e., height of $A_0[p^\infty]^{\text{ét}}$) is at most g. We say that A_0

is *ordinary* when $A_0[p^\infty]$ has the maximal possible p-rank, namely g; equivalently, $A_0[p^\infty]^0$ has height g.

Now assume that A_0 is ordinary. Since

$$A_0^t[p^\infty] \simeq A_0[p^\infty]^t = (A_0[p^\infty]^0)^t \times (A_0[p^\infty]^{\text{ét}})^t$$

with A_0^t isogenous to A_0, for height reasons it follows that the dual of $A_0[p^\infty]^0$ is étale. In other words, if A_0 is ordinary then canonically $A_0[p^\infty] \simeq {X_0'}^t \times X_0$ for étale p-divisible groups X_0 and X_0' that are functorial in $A_0[p^\infty]$. For any complete local noetherian ring R with residue field k, X_0 and X_0' uniquely lift to respective étale p-divisible groups X and X' over R, so the deformation ${X'}^t \times X$ of ${X_0'}^t \times X_0$ corresponds to a canonical formal deformation $\mathfrak{A}$ of A_0 over R. We claim that the formal abelian scheme $\mathfrak{A}$ is algebraic; its algebraization is called the Serre–Tate *canonical lifting.*

Choose a polarization $\phi_0 : A_0 \to A_0^t$. The skew-symmetry of the associated quasi-polarization

$${X_0'}^t \times X_0 = A_0[p^\infty] \to A_0^t[p^\infty] \simeq A_0[p^\infty]^t = X_0^t \times X_0',$$

forces it to have the form $-f_0^t \times f_0$ for a homomorphism $f_0 : X_0 \to X_0'$. There is a unique lifting $f : X \to X'$ of f_0 since X_0 and X_0' are étale, so $-f^t \times f$ lifts $-f_0^t \times f_0$. In other words, the map induced by ϕ_0 between p-divisible groups lifts (necessarily uniquely, by 1.4.4.3) to a homomorphism $\mathfrak{A}[p^\infty] \to \mathfrak{A}^t[p^\infty]$, as suffices for the algebraicity of $\mathfrak{A}$.

Quasi-polarizations yield a p-divisible group analogue of Proposition 1.4.4.14:

1.4.5.5. Theorem. *Let Λ be a complete local noetherian ring with residue field κ of characteristic $p > 0$, let X_0 be a p-divisible group over κ, and let $\alpha_0 : \mathcal{O} \hookrightarrow \mathrm{End}(X_0)$ be an injective homomorphism from an associative finite flat $\mathbb{Z}_p$-algebra. Let $\phi_0 : X_0 \to X_0^t$ be a quasi-polarization of X_0.*

(1) *The functors $\mathrm{Def}_\Lambda(X_0, \alpha_0)$ and $\mathrm{Def}_\Lambda(X_0, \phi_0, \alpha_0)$ on $\mathcal{C}_\Lambda$ are pro-represented by quotients of the deformation ring for $\mathrm{Def}_\Lambda(X_0)$.*
(2) *Let $\Lambda \to \Lambda'$ be a local map between complete local noetherian rings, with $\kappa \to \kappa'$ the induced map between residue fields. Let $(X_0', \phi_0', \alpha_0') = (X_0, \phi_0, \alpha_0)_{\kappa'}$, and let $\mathcal{R}$ and $\mathcal{R}'$ be the respective rings pro-representing $\mathrm{Def}_\Lambda(X_0, \phi_0, \alpha_0)$ and $\mathrm{Def}_{\Lambda'}(X_0', \phi_0', \alpha_0')$. The natural map*

$$\mathcal{R}' \to \Lambda' \widehat{\otimes}_\Lambda \mathcal{R} \tag{1.4.5.2}$$

analogous to (1.4.4.2) is an isomorphism. The same holds for the deformation rings of (X_0, α_0) and (X_0', α_0'), as well as for (X_0, ϕ_0) and (X_0', ϕ_0').

PROOF. Since α_0 is encoded in terms of finitely many endomorphisms of X_0, and ϕ_0 is a homomorphism $X_0 \to X_0^t$, for the proof of (1) it suffices to establish the following general claim (applied to the universal deformation of X_0 and its dual). Let X and Y be p-divisible groups over a complete local noetherian ring $(\mathcal{R}, \mathfrak{m})$ with residue field κ of characteristic p, and let $f_0 : X_0 \to Y_0$ be a homomorphism between the special fibers. We claim there exists an ideal $I \subset \mathcal{R}$ such that for any local map $\mathcal{R} \to R$ to an artinian local ring with residue field κ, a lift $X_R \to Y_R$ of f_0 exists if and only if I has vanishing image in R.

Consider the set-valued functor F on $\mathcal{C}_{\mathcal{R}}$ that carries an object R to the set of all R-homomorphisms $X_R \to Y_R$ lifting f_0 (i.e., $F(R)$ is empty if there is no such lift and $F(R)$ has a single element when a lift exists). The problem is to show that F is pro-represented by a quotient of $\mathcal{R}$. By the functorial aspect of Proposition 1.4.4.11, it is straightforward to check that for a pair of maps $R_1, R_2 \rightrightarrows R_0$ in $\mathcal{C}_{\mathcal{R}}$ at least one of which is surjective, the natural map

$$F(R_1 \times_{R_0} R_2) \to F(R_1) \times_{F(R_0)} F(R_2)$$

is bijective. Moreover, $F(\kappa[\epsilon])$ consists of a single element (the constant deformation of f_0 as a homomorphism from $X \otimes_{\mathcal{R}} \kappa[\epsilon] = X_0 \otimes_\kappa \kappa[\epsilon]$ to $Y_0 \otimes_\kappa \kappa[\epsilon]$), so it vanishes as a κ-vector space. Thus, by Schlessinger's criteria, F is pro-represented by a complete local noetherian $\mathcal{R}$-algebra with residue field κ and has vanishing relative tangent space (over $\mathcal{R}$), so the ring pro-representing F is a quotient of $\mathcal{R}$. This completes the proof of (1).

In view of the proof of (1), to prove (2) it suffices to show that for $(\mathcal{R}, I)$ as above and any local homomorphism $\mathcal{R} \to \mathcal{R}'$ to a complete local noetherian ring with residue field $\kappa' \supset \kappa$, $I\mathcal{R}'$ is the analogous ideal inside $\mathcal{R}'$ relative to $X_{\mathcal{R}'}$, $Y_{\mathcal{R}'}$, and $(f_0)_{\kappa'}$. This seems difficult to verify directly, so we digress to prove an abstract isomorphism criterion for maps such as (1.4.5.2) and then apply it to establish (2).

To formulate an abstract isomorphism criterion for the "change of coefficients" map for deformation rings, we need to assume that the functor is defined on a larger class of rings than the artinian ones. For a complete local noetherian ring Λ with residue field κ, define Inf_Λ to be the category of pairs (Λ', R') consisting of a complete local noetherian Λ-algebra Λ' and a local Λ'-algebra $(R', \mathfrak{m})$ such that

(i) $\Lambda' \to R'$ is local and induces an isomorphism on residue fields,
(ii) $\mathfrak{m}^n = 0$ for some $n \geqslant 1$.

A *morphism* $(\Lambda'_1, R'_1) \to (\Lambda'_2, R'_2)$ consists of a local Λ-algebra map $f : \Lambda'_1 \to \Lambda'_2$ and a local homomorphism $R'_1 \to R'_2$ over f. In an evident way, Inf_Λ contains $\mathcal{C}_{\Lambda'}$ as a full subcategory for any Λ'. Also, if $n \geqslant 1$ and $\{(\Lambda', R'_i)\}$ is a directed system in Inf_Λ such that $\mathfrak{m}^n_{R'_i} = 0$ for all i then $R' := \varinjlim R'_i$ equipped with its evident Λ'-algebra structure is an object in Inf_Λ whose maximal ideal has vanishing nth power. As an important special case, for any (Λ', R') in Inf_Λ with $\mathfrak{m}^n_{R'} = 0$, the directed system $\{R'_i\}$ of artinian local Λ'-subalgebras of R' provides a directed system $\{(\Lambda', R'_i)\}$ in Inf_Λ with all maximal ideals having vanishing nth power and $\varinjlim R'_i = R'$.

Consider a covariant set-valued functor F on Inf_Λ and any directed system $\{(\Lambda', R'_i)\}$ as above. There is a natural map

$$\varinjlim F(\Lambda', R'_i) \to F(\Lambda', \varinjlim R'_i).$$

If this is always bijective then we say that F *commutes with direct limits*. If we only consider such directed systems with a fixed Λ' (such as Λ) then we say F *commutes with direct limits over* Λ'. In each of these definitions it suffices to consider direct limits with R'_i that are artinian. For example, if $(\mathcal{R}, \mathfrak{m})$ is a complete local noetherian Λ-algebra with residue field κ and F is defined to be the functor $(\Lambda', R') \rightsquigarrow \mathrm{Hom}_\Lambda(\mathcal{R}, R')$ (using local Λ-algebra maps) then F commutes with direct limits because $\mathcal{R}/\mathfrak{m}^n$ is artinian with finite Λ-length for every n.

Choose Λ' with residue field κ' and assume the restriction $F|_{\mathcal{C}_{\Lambda'}}$ is pro-represented by a complete local noetherian Λ'-algebra $(\mathcal{R}', \mathfrak{m}')$ with residue field κ'. Also assume $F|_{\mathcal{C}_\Lambda}$ is pro-represented by a complete local noetherian Λ-algebra $(\mathcal{R}, \mathfrak{m})$

with residue field κ. For each $n \geqslant 1$ there is a universal element $\xi_n \in F(\mathcal{R}/\mathfrak{m}^n)$, so for any $m \geqslant 1$ the induced element in $F((\Lambda'/\mathfrak{m}_{\Lambda'}^m) \otimes_\Lambda (\mathcal{R}/\mathfrak{m}^n))$ is classified by a map of local Λ'-algebras

$$\mathcal{R}' \to (\Lambda'/\mathfrak{m}_{\Lambda'}^m) \otimes_\Lambda (\mathcal{R}/\mathfrak{m}^n)$$

that is compatible with change in m and n (since the ξ_n's are compatible with change in n). Passing to the inverse limit defines a map of complete local noetherian Λ'-algebras

$$\mathcal{R}' \to \Lambda' \widehat{\otimes}_\Lambda \mathcal{R} \tag{1.4.5.3}$$

that recovers (1.4.4.2) in the setting of Example 1.4.4.12.

We seek abstract conditions on F which ensure that the map (1.4.5.3) is an isomorphism. Such an isomorphism property for all Λ' (assuming $F|_{\mathcal{C}_{\Lambda'}}$ is pro-represented by a complete local noetherian Λ'-algebra for all Λ') says exactly that $F = \mathrm{Hom}_\Lambda(\mathcal{R}, \cdot)$, since we have seen the necessity of commutation with direct limits in such cases and every object (Λ', R') in Inf_Λ is the direct limit of its artinian local Λ'-subalgebras.

1.4.5.6. Proposition. *Let Λ' be a complete local noetherian Λ-algebra with residue field κ', and let F be a covariant set-valued functor on Inf_Λ such that $F|_{\mathcal{C}_\Lambda}$ and $F|_{\mathcal{C}_{\Lambda'}}$ are pro-represented by complete local noetherian rings $(\mathcal{R}, \mathfrak{m})$ and $(\mathcal{R}', \mathfrak{m}')$ with residue fields κ and κ' respectively. The map (1.4.5.3) is an isomorphism if and only if the following conditions hold:*

(i) *F commutes with direct limits over Λ,*
(ii) *for any $(\Lambda', R') \in \mathcal{C}_{\Lambda'}$ and the local Λ-subalgebra $R = R' \times_{\kappa'} \kappa \subset R'$ with residue field κ, the natural map $F(\Lambda, R) \to F(\Lambda', R')$ is bijective.*

This result is an abstract version of an argument of Faltings in the setting of Galois deformations; see [**129**, pp. 457-8]. Note that R in (ii) is not noetherian when $[\kappa' : \kappa]$ is not finite and $R' \neq \kappa'$.

Proof. The necessity of (i) has been explained, and the necessity of (ii) is obvious. To prove sufficiency, we first make a general construction that has nothing to do with (i) or (ii).

For any (Λ', R') in Inf_Λ, each local Λ-algebra map $f : \mathcal{R} \to R'$ factors through a local Λ-algebra map $f_n : \mathcal{R}/\mathfrak{m}^n \to R'$ for some $n \geqslant 1$. The map

$$F(f_n) : \mathrm{Hom}_\Lambda(\mathcal{R}, \mathcal{R}/\mathfrak{m}^n) = F(\mathcal{R}/\mathfrak{m}^n) \to F(R')$$

produces an element of $F(R')$ that is independent of n and functorial in (Λ', R'), so it defines a natural transformation of functors $\mathrm{Hom}_\Lambda(\mathcal{R}, \cdot) \to F$ on Inf_Λ.

Our problem is precisely to prove that this is an isomorphism on $\mathcal{C}_{\Lambda'}$. By (ii), it suffices to work on the category of pairs (Λ, R). Now using (i), we are done. □

The abstract criteria in Proposition 1.4.5.6 will now be used to establish part (2) of Theorem 1.4.5.5 (taking Λ in the abstract criteria to be the universal deformation ring of X_0 as in Theorem 1.4.5.5). For a pair of p-divisible groups X and Y over Λ and a homomorphism $f_0 : X_0 \to Y_0$ between the special fibers, define the covariant set-valued functor F on Inf_Λ to carry (Λ', R') to the set of deformations of $(f_0)_{\kappa'}$ to R' (where κ' is the residue field of Λ'). The set $F(\Lambda', R')$ is empty when there is no lift and it consists of a single element when there exists a lift and R' is artinian (as the uniqueness of such a lift for artinian R' follows from Proposition 1.4.4.3). In fact $F(\Lambda', R')$ always consists of a single element when it is non-empty, even when R' is not noetherian. The key point is that $\mathfrak{m}^n = 0$ for some $n \geqslant 1$, so we can apply:

1.4.5.7. Lemma. *Let R be a ring in which a prime p is nilpotent and let $J \subset R$ be an ideal such that $J^n = 0$ with $n \geqslant 1$. Let $f : X \to Y$ be a homomorphism between p-divisible groups over R. If f vanishes modulo J then $f = 0$.*

Proof. The case $n = 1$ is trivial, and by induction on n we may assume $n = 2$. Our problem is comparing two R-homomorphisms with the same reduction modulo J. Equipping J with trivial divided powers, this problem will be solved used Grothendieck–Messing theory. Consider the Lie algebras of the universal vector extensions $\mathrm{E}(X)$ and $\mathrm{E}(Y)$, equipped with their respective Hodge subbundles $\mathrm{Lie}(X^t)^\vee$ and $\mathrm{Lie}(Y^t)^\vee$. For any R-homomorphism $u : X \to Y$, Grothendieck–Messing theory shows that the map $\mathrm{Lie}(\mathrm{E}(u))$ respecting Hodge subbundles uniquely determines u and only depends on $u_0 := u \bmod J$. Hence, if $u_0 = 0$ then $u = 0$. □

We now apply Proposition 1.4.5.6 to the functor F defined above whose value on any $(\Lambda', R') \in \mathrm{Inf}_\Lambda$ is empty or a singleton. The established part (1) of Theorem 1.4.5.5 (with varying Λ) implies the pro-representability hypothesis in Proposition 1.4.5.6. Thus, we just have to verify conditions (i) and (ii) in Proposition 1.4.5.6. Condition (ii) is immediate via Proposition 1.4.4.11. To establish (i) for $(\Lambda', R') = \varinjlim(\Lambda', R'_i)$, we just have to show that if $F(\Lambda', R')$ is non-empty then so is $F(\Lambda', R'_i)$ for some i. We may rename Λ' as Λ, R' as R, and R'_i as R_i for simplicity of notation. Our problem is to show that if f_0 lifts to an R-homomorphism $f : X_R \to Y_R$ then f descends to an R_i-homomorphism $X_{R_i} \to Y_{R_i}$ for some large i. We shall induct on the integer $n \geqslant 1$ such that the maximal ideal $\mathfrak{m}$ of R and maximal ideal $\mathfrak{m}_i$ of every R_i have vanishing nth power, the case $n = 1$ being trivial.

Let $\overline{R} = R/\mathfrak{m}^{n-1}$ and $\overline{R}_i = R_i/\mathfrak{m}_i^{n-1}$, so $\varinjlim \overline{R}_i = \overline{R}$. We may assume $n \geqslant 2$ and (by induction) that the lift $\overline{f} := f_{\overline{R}}$ of f_0 descends to a (necessarily unique) lift $\overline{f}_{i_0} : X_{\overline{R}_{i_0}} \to Y_{\overline{R}_{i_0}}$ of f_0. For $i \geqslant i_0$ let $\overline{f}_i = \overline{f}_{i_0} \otimes_{\overline{R}_{i_0}} \overline{R}_i$. For $i \geqslant i_0$, if there is a lift $f_i : X_{R_i} \to Y_{R_i}$ of $\overline{f}_i$ then $f_i \otimes_{R_i} R$ is a lift of f_0 and thus coincides with f (by Lemma 1.4.5.7). Hence, it is necessary and sufficient to find $i \geqslant i_0$ so that $\overline{f}_i$ lifts over R_i.

By Grothendieck–Messing theory (see [**75**, IV, 2.5; V, 1.6]), for every $i \geqslant i_0$ there is a canonical map

$$L_i : \mathrm{Lie}(\mathrm{E}(X_{R_i})) \to \mathrm{Lie}(\mathrm{E}(Y_{R_i}))$$

that only depends on $\overline{f}_i$ and has reduction $\mathrm{Lie}(\mathrm{E}(\overline{f}_i))$ modulo the square-zero ideal $\mathfrak{m}_i^{n-1} \subset R_i$, and moreover L_i respects the Hodge subbundles if and only if $\overline{f}_i$ lifts to an R_i-homomorphism $X_{R_i} \to Y_{R_i}$. Thus, it is necessary and sufficient to prove that L_i respects the Hodge subbundles for large i. Compatibility with base change ensures that $L_{i'} = L_i \otimes_{R_i} R_{i'}$ whenever $i' \geqslant i \geqslant i_0$ and that $L_i \otimes_{R_i} R = \mathrm{Lie}(\mathrm{E}(f))$. But this latter map respects the Hodge subbundles since it arises from an R-homomorphism f lifting $\overline{f}$. Hence, by standard limit arguments (and the compatibility of the Hodge subbundles with respect to base change) it follows that L_i respects the Hodge subbundles for sufficiently large i. This completes the proof of Theorem 1.4.5.5. □

1.5. CM types

Let A be an isotypic abelian variety of dimension $g > 0$ over a field K such that A admits sufficiently many complex multiplications. By Theorem 1.3.4, we may and do choose a CM field $L \subset \mathrm{End}^0(A)$ with degree $2g$. (Conversely, by Theorem 1.3.1.1, the existence of such an L forces A to be isotypic.) It turns out that the L-linear isogeny class of A is encoded in terms of a rather simple discrete invariant when $\mathrm{char}(K) = 0$ and K is algebraically closed. We wish to review the basic features of this invariant, called the CM type, and to discuss some useful replacements for it in positive characteristic.

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

1.5.1. Characteristic 0. We now focus on the case $\mathrm{char}(K) = 0$. Let K'/K be an algebraically closed extension. Since $L \otimes_{\mathbb{Q}} K \simeq \prod K_i$ for finite (separable) extensions K_i/K, any $L \otimes_{\mathbb{Q}} K$-module M canonically decomposes as $\prod M_i$ for a K_i-vector space M_i. Thus, if $\dim_K M$ is finite then the isomorphism class of M is determined by the numbers $\dim_{K_i} M_i$, which in turn are determined by the isomorphism class of the $L \otimes_{\mathbb{Q}} K'$-module $M \otimes_K K'$.

The K'-algebra $L \otimes_{\mathbb{Q}} K'$ has a very simple form: it is $\prod_{\varphi} K'_{\varphi}$ where φ ranges through all field embeddings $L \to K'$ and K'_{φ} denotes K' viewed as an L-algebra via φ. Hence, any $L \otimes_{\mathbb{Q}} K'$-module M' decomposes into a corresponding product of eigenspaces M'_{φ} over K' on which L acts through φ. We conclude that for an $L \otimes_{\mathbb{Q}} K$-module M with finite K-dimension, the isomorphism class of M is determined by the numbers $\dim_{K'}(M \otimes_K K')_{\varphi}$ as φ varies through $\mathrm{Hom}(L, K')$.

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

An especially interesting example is the $L \otimes_{\mathbb{Q}} K'$-module $M = T \otimes_K K'$ with $T = \mathrm{Lie}(A)$ for a CM abelian variety A over K with complex multiplication by L. There is a non-trivial constraint on the eigenspaces $(T \otimes_K K')_{\varphi}$ for the L-action on $T \otimes_K K'$ (with φ varying through the embeddings $\varphi : L \to K'$):

1.5.2. Lemma. *When* $\mathrm{char}(K) = 0$*, each eigenspace* $(T \otimes_K K')_{\varphi}$ *is at most* 1*-dimensional over* K'*. If* Φ *denotes the set of* g *distinct embeddings* $\varphi : L \to K'$ *for which there is a* φ*-eigenline in* $T \otimes_K K'$ *then* Φ *contains no "conjugate pairs". That is, we have a disjoint union decomposition* $\mathrm{Hom}(L, K') = \Phi \coprod (\Phi \circ \iota)$.

PROOF. By considerations with direct limits (as in the proof of Proposition 1.2.6.1), we may and do first arrange that K is finitely generated over $\mathbb{Q}$. The choice of algebraically closed extension K'/K does not matter, so we can replace

K' with $\overline{K}$. We may then reduce to the case $K = K' = \mathbb{C}$, in which case a proof is given via the complex-analytic uniformization in [**82**, §22]. □

The preceding considerations motivate the following concepts.

1.5.2.1. Definition. (i) Let L be a CM field of degree $2g$ over $\mathbb{Q}$ and K an algebraically closed field of characteristic 0. An K-valued CM *type* for L is a subset $\Phi \subset \mathrm{Hom}(L, K)$ of representatives for the g orbits of the action by the complex conjugation ι of L. That is, Φ consists of g distinct elements such that $\varphi \circ \iota \notin \Phi$ for all $\varphi \in \Phi$, or equivalently $\mathrm{Hom}(L, K) = \Phi \coprod (\Phi \circ \iota)$. To emphasize the role of L, we often refer to the pair (L, Φ) as a CM *type*.

(ii) Let $L = L_1 \times \cdots \times L_s$ be a CM algebra, where each L_i is a CM field. A CM *type* for L is a subset $\coprod \Phi_i \subset \coprod \mathrm{Hom}(L_i, K) = \mathrm{Hom}(L, K)$ where (L_i, Φ_i) is a CM type for each i.

If K is a field of characteristic 0 and K'/K is an algebraically closed extension, then the tangent space to a CM abelian variety A over K with complex multiplication by a CM algebra L determines a K'-valued CM type Φ for L (apply Lemma 1.5.2 to the isogeny factors of A determined by the primitive idempotents of L). This is an invariant of the L-linear isogeny class of A over K.

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

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

In the complex-analytic theory [**82**, §22] it is proved (using that L is a CM field) that this complex torus admits a Riemann form (with respect to which the action of each $c \in L$ has adjoint given by the complex conjugate $\overline{c} \in L$), and hence is an abelian variety. Let A_Φ be the corresponding abelian variety over $\mathbb{C}$. By construction (and GAGA), we get an action by $\mathcal{O}_L$ on A_Φ and hence an embedding $L \hookrightarrow \mathrm{End}^0(A_\Phi)$ as a subfield of $\mathbb{Q}$-degree $[L : \mathbb{Q}] = 2\dim(A_\Phi)$. This makes A_Φ into a CM abelian variety over $\mathbb{C}$ with complex multiplication by L. The action by any $c \in \mathcal{O}_L \subset \mathrm{End}(A_\Phi)$ on

$$\mathrm{Lie}(A_\Phi) = \mathrm{Lie}(A_\Phi^{\mathrm{an}}) = (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi = \prod_{\varphi \in \Phi} \mathbb{C}_\varphi$$

is the map $(a_\varphi) \mapsto (\varphi(c) a_\varphi)$ involving multiplication in $\mathbb{C}$. Thus, A_Φ equipped with the embedding $L \hookrightarrow \mathrm{End}^0(A_\Phi)$ gives rise to the CM type Φ on L.

The CM abelian varieties A_Φ are generally not simple; see Remark 1.5.4.2 for further discussion of the simplicity aspect. It is shown in the classical theory [**82**, §22, First Ex., Thm.] that as we vary Φ through all CM types on L, the A_Φ vary (without repetition) through all L-linear isogeny classes of (necessarily isotypic) CM abelian varieties over $\mathbb{C}$ with complex multiplication by L.

1.5.3.1. Definition. Let A be an isotypic abelian variety of dimension $g > 0$ over a field K, and let L be a CM field of degree $2g$ equipped with an embedding $j : L \hookrightarrow \mathrm{End}^0(A)$. The *dual* CM *structure* on the dual abelian variety A^t is the embedding $L \hookrightarrow \mathrm{End}^0(A^t)$ defined by $x \mapsto j(\overline{x})^t$, where $x \mapsto \overline{x}$ is complex conjugation on L.

It is easy to check that this definition respects double duality (i.e., if A^{tt} is equipped with the CM structure dual to the one on A^t then the canonical isomorphism $A \simeq A^{tt}$ is L-linear). The reason for the appearance of complex conjugation on L in the definition of the dual CM structure is that when K is algebraically closed of characteristic 0 it gives A^t the *same* (K-valued) CM type as A.

To verify this equality of CM types we may reduce to the case when $K = \mathbb{C}$ and then use the exhaustive construction in the complex-analytic theory as in Example 1.5.3. Alternatively, still working over $\mathbb{C}$, consider the functorial isomorphism $\mathrm{Lie}(A^t) \simeq \mathrm{H}^1(A, \mathcal{O}_A)$ and the functorial Hodge decomposition

$$\mathbb{C} \otimes_{\mathbb{Q}} \mathrm{H}_1(A(\mathbb{C}), \mathbb{Q}) \simeq \mathrm{H}^1(A(\mathbb{C}), \mathbb{C})^\vee \simeq \mathrm{Lie}(A) \oplus \mathrm{H}^1(A, \mathcal{O}_A)^\vee.$$

Since $\mathrm{H}_1(A(\mathbb{C}), \mathbb{Q})$ is 1-dimensional as an L-vector space, when A^t is equipped with the dual action $j(x)^t$ (without the intervention of complex conjugation) then its CM type is $\mathrm{Hom}(L, \mathbb{C}) - \Phi = \overline{\Phi}$.

1.5.4. Descent to a number field. For a CM abelian variety over an algebraically closed field K of characteristic 0, we may make the CM type essentially be independent of K by replacing K with $\overline{\mathbb{Q}}$ (see Remark 1.5.2.2). This enables us to use the complex-analytic theory to prove the following purely algebraic result.

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

The hypothesis $K = \overline{K}$ cannot be weakened. For example, if K is a number field containing a Galois closure of L over $\mathbb{Q}$ (so all $\overline{K}$-valued CM types on L are K-valued) then any quadratic twist of A (equipped with the evident L-linear structure) has the same CM type as (A, j) but is generally not K-isogenous to A.

Proof. In view of Lemma 1.2.1.2, by expressing K as a direct limit of algebraically closed subfields of finite transcendence degree over $\mathbb{Q}$ we can reduce to the case when K has finite transcendence degree over $\mathbb{Q}$. To show that the CM type determines the L-linear isogeny class it suffices (again by Lemma 1.2.1.2) to treat the case $K = \mathbb{C}$. This case was addressed in Example 1.5.3 via the complex-analytic theory, where it was also seen that every CM type Φ on L does arise when $K = \mathbb{C}$.

It remains to show that every CM type Φ on L arises when $K = \overline{\mathbb{Q}}$. Consider the CM abelian variety A_Φ over $\mathbb{C}$ with complex multiplication by L and CM type Φ as in Example 1.5.3. Recall that $\mathcal{O}_L = L \cap \mathrm{End}(A_\Phi)$ inside $\mathrm{End}^0(A_\Phi)$. By expressing $\mathbb{C}$ as a direct limit of its finitely generated $\overline{\mathbb{Q}}$-subalgebras, there is such a subalgebra R for which A with its $\mathcal{O}_L$-action over $\mathbb{C}$ descends to an abelian scheme $\mathscr{A}$ over R equipped with an $\mathcal{O}_L$-action.

By localization of R, we can arrange that the tangent space $\mathrm{Lie}(\mathscr{A})$ is finite and free as an R-module, and by increasing R to contain the integer ring of the Galois closure of L in $\mathbb{C}$ we can arrange that the $\mathcal{O}_L$-action on $\mathrm{Lie}(\mathscr{A})$ decomposes as $\prod_{\varphi\in\Phi} R_\varphi$ with R_φ equal to R having action by $c \in \mathcal{O}_L$ through multiplication by $\varphi(c) \in \overline{\mathbb{Q}} \subset R$. For any maximal ideal $\mathfrak{m}$ of R, the natural map of $\overline{\mathbb{Q}}$-algebras $\overline{\mathbb{Q}} \to R/\mathfrak{m}$ is an isomorphism. Thus, passing to the fiber of $\mathscr{A}$ at a closed point of $\mathrm{Spec}(R)$ gives a pair (A, j) over $\overline{\mathbb{Q}}$ with CM type Φ. □

This proposition has an important consequence for descending the field of definition of a CM abelian variety in characteristic 0, as we will see in Theorem 1.7.2.1.

1.5.4.2. Remark. By Theorem 1.3.1.1, for any (A, L) as in Proposition 1.5.4.1, A has a unique simple factor C (in the sense of Definition 1.2.1.5). By Proposition 1.3.2.1, C is a CM abelian variety with complex multiplication by the CM field $L' := \mathrm{End}^0(C)$ (see Proposition 1.3.6.4(1)). Since L' is canonically identified with the center of $\mathrm{End}^0(A)$, it naturally embeds into L. Hence, there is a K-valued CM type Ψ on L' arising from C, and the pair (L', Ψ) is determined by (L, Φ) since A with its complex multiplication by L is determined up to L-linear isogeny by Φ (and $L' = L$ if and only if $A = C$, which is to say that A is simple). It is therefore natural to seek an intrinsic recipe to directly construct (L', Ψ) from (L, Φ), and in particular to characterize in terms of Φ whether or not A is simple.

The criterion is this: among the CM fields in L from which Φ is obtained by full preimage under restriction, (L', Ψ) is the unique such pair with $[L' : \mathbb{Q}]$ minimal and Φ the full preimage of Ψ. Indeed, since the CM type is $\overline{\mathbb{Q}}$-valued (Remark 1.5.2.2) and the base field K is algebraically closed, it suffices to treat the case $K = \mathbb{C}$. In this case the desired recipe is established in the complex-analytic theory (see [**82**, §22, Rem. (1)]).

1.5.5. Positive characteristic. Assume $\mathrm{char}(K) > 0$, and let A be an abelian variety over K of dimension $g > 0$ admitting an action by an order $\mathcal{O}$ in a CM field L of degree $2g$ over $\mathbb{Q}$. There is no action by $L = \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}$ on the tangent space $T := \mathrm{Lie}(A)$ of A at the origin since L is a $\mathbb{Q}$-algebra and T is a K-vector space. Thus, there is not a good notion of CM type on L associated to the embedding of L into $\mathrm{End}^0(A)$. More specifically, for the CM order $\mathcal{O} := L \cap \mathrm{End}(A)$ in L, T has a K-linear action by $\mathcal{O}/(p)$ and there is generally no constraint on this action akin to the eigenspace decomposition considered in characteristic 0 (as in Lemma 1.5.2). The lack of such a constraint occurs for a couple of reasons, as we now explain.

1.5.5.1. Example. If p divides the discriminant of $\mathcal{O}$ over $\mathbb{Z}$ or $p\mathcal{O}_L$ is not prime in $\mathcal{O}_L$ then $\mathcal{O}/p\mathcal{O}$ fails to be a field. In such cases, the K-linear $\mathcal{O}/(p)$-action on T admits no notion of eigenspace decomposition that closely resembles the situation in characteristic 0.

1.5.5.2. Example. Suppose that $\mathcal{O}$ has discriminant not divisible by p (so $\mathcal{O}_{(p)} = \mathcal{O}_{L,(p)}$) and that p is totally inert in L. In such cases $\kappa := \mathcal{O}/(p)$ is a finite field of degree $2g$ over $\mathbb{F}_p$ and $\mathrm{Aut}(L/\mathbb{Q})$ injects into $\mathrm{Gal}(\kappa/\mathbb{F}_p)$, so the canonical complex conjugation on L induces a non-trivial involution on κ.

For an algebraically closed extension K'/K we can consider the eigenspace decomposition of $T \otimes_K K'$ over $\kappa \otimes_{\mathbb{F}_p} K' = \prod_\varphi K'_\varphi$ where φ ranges over the $2g$ distinct embeddings of κ into K'. This could fail to resemble the CM types that arise in characteristic 0 because (as we shall see in later examples, such as in Remark 2.3.4) there may be conjugate pairs occurring among the φ for which $T \otimes_K K'$ has a non-zero φ-eigenspace with respect to its K'-linear κ-action.

In such cases, the composite action

$$\mathcal{O} \to \mathrm{End}(A) \to \mathrm{End}(A)/(p) \to \mathrm{End}_K(T)$$

does not "look like the reduction of a CM type", and so this provides an obstruction for A equipped with its $\mathcal{O}$-action to lift to characteristic 0. There is no dimension obstruction to such lifting: each φ-eigenspace in $T \otimes_K K' = \mathrm{Lie}(A_{K'})$ has K'-dimension at most 1. To prove this, first note that the Dieudonné module $D := \mathrm{M}^*(A_{K'}[p^\infty])$ is free of rank 1 over

$$\mathcal{O} \otimes_{\mathbb{Z}} W(K') = \mathcal{O}_{(p)} \otimes_{\mathbb{Z}_{(p)}} W(K') = \mathcal{O}_L \otimes_{\mathbb{Z}} W(K')$$

by Proposition 1.4.3.9(2) (or Proposition 1.2.5.1 and $W(K')$-rank considerations), so D/pD is free of rank 1 over $\kappa \otimes_{\mathbb{F}_p} K'$. The formal group $\widehat{A}_{K'}$ is the identity component of the p-divisible group $A_{K'}[p^\infty]$ (Example 1.4.3.6), and its tangent space coincides with that of $A_{K'}$. Hence, by 1.4.3.2(4),

$$T \otimes_K K' \simeq \mathrm{Lie}(A_{K'}[p^\infty]) \simeq (D/\mathcal{F}(D))^\vee,$$

where $\mathcal{F} : D \to D$ denotes the semilinear Frobenius endomorphism. By naturality, this composite isomorphism is $\kappa \otimes_{\mathbb{F}_p} K'$-linear, so $T \otimes_K K'$ is monogenic over $\kappa \otimes_{\mathbb{F}_p} K'$ since the K'-linear dual of a monogenic $\kappa \otimes_{\mathbb{F}_p} K'$-module is monogenic (as $\kappa \otimes_{\mathbb{F}_p} K'$ is a finite étale K'-algebra). Each φ-eigenspace of $T \otimes_K K'$ is therefore monogenic over K', which is to say is of dimension at most 1 over K'.

To go beyond Example 1.5.5.2, an obstruction to the existence of a CM lift over a *normal* local domain of characteristic 0 will be formulated precisely later (see 2.1.5 and 4.1.2). This will be used to exhibit examples (e.g., in 4.1.2) of abelian varieties over finite fields for which there is no such lift. Such examples are interesting due to Corollary 1.6.2.5 below, according to which *every* abelian variety over a finite field admits sufficiently many complex multiplications.

Although the Lie algebra fails to be an isogeny invariant for the study of CM abelian varieties in positive characteristic (and $\mathrm{End}^0(A)$ does not act on the tangent space when $\mathrm{char}(K) > 0$), there is an alternative linear object attached to a CM abelian variety A that serves as a good substitute when $\mathrm{char}(K) = p > 0$: the p-divisible group $A[p^\infty]$, or its (contravariant) Dieudonné module $\mathrm{M}^*(A[p^\infty])$ when K is perfect.

Letting $B = A$ in Proposition 1.2.5.1, we see that $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}(A)$ acts faithfully on $A[p^\infty]$. Hence, $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{End}^0(A)$ acts faithfully on $A[p^\infty]$ in the isogeny category of p-divisible groups over K. In particular, if K is perfect (e.g., finite) and A is an isotypic CM abelian variety over K with complex multiplication by the CM field L (see Theorem 1.3.4) then $L_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} L$ acts faithfully and linearly on the vector space $\mathrm{M}^*(A[p^\infty])[1/p]$ of rank $2g$ over the absolutely unramified p-adic field $W(K)[1/p]$.

This $W(K)[1/p]$-linear faithful L_p-action for perfect K with $\mathrm{char}(K) = p$ is an analogue of a classical construction when $\mathrm{char}(K) = 0$: the action of L on the algebraic de Rham cohomology $\mathrm{H}^1_{\mathrm{dR}}(A/K)$ (a filtered K-vector space of dimension $2g$). It will be useful in later considerations (e.g., the proof of Theorem 2.2.3) with lifting problems from positive characteristic to characteristic 0. (Note that when $\mathrm{char}(K) = 0$, $\mathrm{H}^1_{\mathrm{dR}}(A/K)$ provides essentially the same information as the CM type arising from the L-action on $\mathrm{Lie}(A) = \mathrm{H}^0(A, \Omega^1_{A/K})^\vee$, in view of the Hodge filtration on $\mathrm{H}^1_{\mathrm{dR}}(A/K)$; cf. Definition 1.5.3.1 and the subsequent discussion there.)

1.6. Abelian varieties over finite fields

In this section we work over a finite field κ with $\mathrm{char}(\kappa) = p$.

1.6.1. Tate's theorem and Weil numbers. A fundamental fact in the theory of abelian varieties over finite fields is:

1.6.1.1. Theorem (Tate's isogeny theorem)**.** *For abelian varieties A and B over a finite field κ, the natural injective map*

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

is bijective for every prime ℓ (including $\ell = \mathrm{char}(\kappa)$).

Proof. By passing to $A \times B$, it suffices to treat the case $A = B$, as we shall now consider. The case $\ell \neq \mathrm{char}(\kappa)$ is the main result in [**118**]; see [**82**, App. I, Thm. 1] for a proof as well. Unfortunately, Tate did not publish his proof for the case $\ell = p$ (though his argument was published in [**79**]). See Appendix A.1 for a proof. □

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

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

is central in D since the q-Frobenius is functorial on the category of κ-schemes. Hence, the number field $\mathbb{Q}[\pi] = \mathbb{Q}(\pi)$ is contained in the center of D.

Even without simplicity or isotypicity hypotheses on A, Tate proved (see [**82**, App. I, Thm. 3(a)]) that the commutative $\mathbb{Q}$-algebra $\mathbb{Q}[\pi]$ is the center of $\mathrm{End}^0(A)$ for any abelian variety A over κ.

1.6.1.2. Definition. Let $q = p^n$ for a positive integer n and prime number p. Let F be a field of characteristic 0.

(i) A *Weil q-integer* in F (or a *Weil q-integer of weight* 1, to be precise) is an algebraic integer $z \in F$ whose $\mathbb{Q}$-conjugates in $\mathbb{C}$ have absolute value $q^{1/2}$.[2]

(ii) Let w be an integer. A *Weil q-number* of weight w is an algebraic number z such that $\mathrm{ord}_v(z) = 0$ for all finite places v of $\mathbb{Q}(z)$ prime to q and $|\tau(y)| = q^{w/2}$ for all injective ring homomorphisms $\tau\colon \mathbb{Q}(z) \to \mathbb{C}$.

Note that a Weil q-integer as defined above is precisely a Weil q-number of weight 1 such that $\mathrm{ord}_v(z) \geqslant 0$ for all p-adic places v of $\mathbb{Q}(z)$. The interest in Definition 1.6.1.2 is that Weil proved (see [**95**, §3]) that for any non-zero abelian

[2]What is called a Weil q-integer here is often called a "Weil q-number" or "Weil q-number of weight 1" in the literature.

variety A over κ and any $\ell \neq p := \mathrm{char}(\kappa)$, the $\mathbb{Q}_\ell$-linear q-Frobenius action on $V_\ell(A)$ has characteristic polynomial $f_{A,q} \in \mathbb{Z}[T]$ that is independent of ℓ and has all roots in $\mathbb{C}$ equal to Weil q-integers.

In Tate's work, he also proved (see [**82**, App. I, Thm. 3(e)]) that A is isotypic if and only if the common characteristic polynomial $f_{A,q} \in \mathbb{Z}[T]$ of the q-Frobenius action on the Tate modules has a single monic irreducible factor over $\mathbb{Q}$, in which case this irreducible factor is obviously the minimal polynomial f_π over $\mathbb{Q}$ for the q-Frobenius endomorphism $\pi \in \mathrm{End}^0(A)$ (since π is central). The polynomial f_π only depends on A through its isogeny class (due to the functoriality of q-Frobenius on κ-schemes), and by Weil's Riemann Hypothesis its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy class of roots in $\mathbb{C}$ consists of Weil q-integers, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

1.6.2. The Honda-Tate theorem. Fix an abstract algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let $\mathrm{Weil}(q)$ denote the set of Weil q-integers in $\overline{\mathbb{Q}}$. Elements of $\mathrm{Weil}(q)$ are *equivalent* when they lie in the same $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit; i.e., they have the same minimal polynomial over $\mathbb{Q}$. The following remarkable result relates Weil q-integers to isogeny classes of simple abelian varieties over a finite field of size q.

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

PROOF. We refer the reader to [**50**], [**121**], and [**95**] for a discussion of the proof of the Honda-Tate theorem. The proof of injectivity in Theorem 1.6.2.1 rests on the work of Tate related to Theorem 1.6.1.1. The proof of surjectivity uses abelian varieties in characteristic 0 (in fact, it uses descents to number fields of CM abelian varieties over $\mathbb{C}$; see Theorem 1.7.2.1). We are not aware of a proof of surjectivity that avoids abelian varieties in characteristic 0. □

The following consequence of the (proof of the) Honda–Tate theorem describes the possibilities for the division algebra $D = \mathrm{End}^0(A)$ in terms of whether the center Z is $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$ (the totally real cases) or a CM field.

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

(1) *We have $\pi^2 = q = p^n$ with n even. This is precisely the case $Z = \mathbb{Q}$, and occurs exactly when D is a central quaternion division algebra over $\mathbb{Q}$, in which case it is the unique quaternion division algebra over $\mathbb{Q}$ ramified at exactly $\{p, \infty\}$.*

 Each of the isogeny classes of simple abelian varieties with $\pi \in \{\pm p^{n/2}\}$ consists of supersingular elliptic curves E over κ for which all endomorphisms of $E_{\overline{\kappa}}$ are defined over κ (equivalently, the geometric endomorphism algebra $\mathrm{End}^0(E_{\overline{\kappa}})$ *coincides with* $\mathrm{End}^0(E)$*).*

(2) *We have $\pi^2 = q = p^n$ with n odd. This is precisely the case $Z = \mathbb{Q}(\sqrt{p})$, and occurs if and only if D is the unique central quaternion division algebra over Z ramified at exactly the two infinite places of Z.*

 The corresponding isogeny class of simple abelian varieties is represented by the 2-dimensional Weil restriction $\mathrm{Res}_{\kappa'/\kappa}(E')$ *where κ'/κ is a quadratic extension and E' is a supersingular elliptic curve over κ' whose geometric endomorphism algebra is defined over κ'.*

(3) *The field Z is a* CM *field. In such cases, D is the central division algebra over Z that is split at all places of Z away from p and for each p-adic place v of Z has local invariant* $\mathrm{inv}_v(D) = (\mathrm{ord}_v(\pi)/\mathrm{ord}_v(q))[Z_v : \mathbb{Q}_p] \bmod \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$.

The members of the corresponding isogeny class of simple abelian varieties over κ have dimension $g = (1/2)[Z : \mathbb{Q}] \cdot \sqrt{[D : Z]}$.

Proof. Since π is a Weil q-integer, for any embedding $j : Z \to \mathbb{C}$ the subfield $j(Z)$ in $\mathbb{C}$ is stable under complex conjugation and the effect of this involution on Z is given by the intrinsic formula $\pi \mapsto q/\pi$ that is independent of j. Thus, Z is either totally real or a CM field and the totally real cases are precisely when $\pi^2 = q = p^n$, with $Z = \mathbb{Q}$ for even n and $Z = \mathbb{Q}(\sqrt{p})$ for odd n.

In all cases, D is split at the finite places of Z away from p. Indeed, Tate's isogeny theorem away from p implies that for a prime $\ell \neq p$ the map

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} D \to \mathrm{End}_{Z_\ell}(V_\ell(A)) \tag{1.6.2.1}$$

is an isomorphism (using that the Z-action on $V_\ell(A)$ encodes the action of the Galois group $\mathrm{Gal}(\overline{\kappa}/\kappa)$). The right side of (1.6.2.1) is visibly a product of matrix algebras over factor fields of $Z_\ell = \prod_{v|\ell} Z_v$, so D splits at all ℓ-adic places of Z. Writing $d^2 = [D : Z]$, the Z_v-algebra isomorphism $D_v \simeq \mathrm{End}_{Z_v}(V_v(A))$ for $v|\ell$ implies that $V_v(A)$ has Z_v-dimension d for all such v, so $V_\ell(A)$ is free of rank d over Z_ℓ. Hence, $[Z_\ell : \mathbb{Q}_\ell]d = 2g$, so $g = (1/2)[Z : \mathbb{Q}]\sqrt{[D : Z]}$. This is the asserted dimension formula in case (3), and the proof also applies in cases (1) and (2) (as will be used below). The formula for $\mathrm{inv}_v(D)$ in case (3) with $v|p$ is proved in A.1.3, resting on preliminary work in A.1.1 and A.1.2, and that proof is applicable regardless of whether Z is CM or totally real. This completes the proof of case (3), and in cases (1) and (2) (so $\pi^2 = q$) it establishes the formula $\mathrm{inv}_v(D) = [Z_v : \mathbb{Q}_p]/2 \bmod \mathbb{Z}$ for p-adic places v of Z.

Consider case (1) (equivalently, $\pi = \pm p^{n/2}$ with n even), so D is a central division algebra over $Z = \mathbb{Q}$ split away from p and ∞ with $\mathrm{inv}_p(D) = 1/2 \bmod \mathbb{Z}$. This forces $\mathrm{inv}_\infty(D) = 1/2 \bmod \mathbb{Z}$, so D is a quaternion division algebra over $\mathbb{Q}$. In particular, the dimension formula yields $g = 1$, so A is an elliptic curve. In view of the other possibilities for Z, these are the only cases for which D is a central quaternion division algebra over $\mathbb{Q}$. The elliptic curves E that arise in such cases must be supersingular (since it is classical that $\mathrm{End}^0(E_{\overline{\kappa}})$ is commutative in the ordinary case). Moreover, since it is classical that $\mathrm{End}^0(E_{\overline{\kappa}})$ is a quaternion division algebra in the supersingular case, it follows for $\mathbb{Q}$-dimension reasons that the injection $D = \mathrm{End}^0(E) \to \mathrm{End}^0(E_{\overline{\kappa}})$ is an equality. In other words, all endomorphisms of $E_{\overline{\kappa}}$ are defined over κ. This settles case (1).

Finally, consider case (2). Since the numbers $\pm p^{n/2}$ with odd n are Galois conjugate over $\mathbb{Q}$, there is exactly one isogeny class that arises in this case. For the unique p-adic place v of $Z = \mathbb{Q}(\sqrt{p})$, the formula for $\mathrm{inv}_v(D)$ vanishes. Hence, D splits away from the two real places of Z, so its order in $\mathrm{Br}(Z)$ divides 2 and the dimension formula says $g = \sqrt{[D : Z]}$. Thus, either $D = Z$ and A is an elliptic curve or D is the unique central quaternion division algebra over Z split away from the real places and A is an abelian surface. The first case cannot happen, since otherwise the quadratic field Z would provide a CM structure on the elliptic curve, contradicting Proposition 1.3.6.4(2) since $D = Z$ is a real quadratic field.

For the quadratic extension κ' of κ, the abelian surface $A_{\kappa'}$ is isotypic (by 1.2.6.1). But its q^2-Frobenius is $\pi_{\kappa'}^2 = q$, which by the settled case (1) over κ' is the Weil q^2-integer associated to some supersingular elliptic curve over κ'. Hence, $A_{\kappa'}$ cannot also be κ'-simple, so it is isogenous to $E' \times E'$ for an elliptic curve E' over κ' that must be in the isogeny class which occurs in case (1) over κ'. Choosing such an isogeny decomposition provides a non-zero homomorphism $A_{\kappa'} \to E'$ over κ'. By the universal property of Weil restriction, we thereby get a non-zero κ-homomorphism $A \to \mathrm{Res}_{\kappa'/\kappa}(E')$. Since A is κ-simple, by dimension reasons this must be an isogeny. The existence of A is guaranteed by the Honda–Tate classification, so it follows that for E' as in case (1) over κ', the abelian surface $\mathrm{Res}_{\kappa'/\kappa}(E')$ is necessarily κ-simple and lies in the unique isogeny class occurring in case (2) over κ. □

1.6.2.3. Remark. In the terminology of Theorem 1.3.6.2, the three cases in Corollary 1.6.2.2 correspond to A that are respectively of Type III with $e = 1$, Type III with $e = 2$, and Type IV. We saw in the proof of 1.6.2.2 that the formula for $\mathrm{inv}_v(D)$ for p-adic places v of Z in case (3) works in cases (1) and (2), and that the dimension formula in case (3) works in cases (1) and (2) (though these facts in cases (1) and (2) are also clear by inspection).

The common $\mathbb{Q}$-degree $[Z : \mathbb{Q}]\sqrt{[D : Z]}$ of maximal commutative subfields of the division algebra D is $2g$ in each case of Corollary 1.6.2.2, so *simple* abelian varieties over finite fields always have sufficiently many complex multiplications.

1.6.2.4. Example. Observe that in part (3) of Corollary 1.6.2.2, for any elliptic curve case that arises necessarily the CM field $Z = \mathbb{Q}[\pi]$ is imaginary quadratic and $D = Z$. Writing $q = p^r$, the elliptic curves that arise in this way are as follows, depending on the behavior of p in the imaginary quadratic field $Z = \mathbb{Q}[\pi]$.

There are several possibilities for the splitting behavior of p in Z: (i) p splits in Z with π generating the rth power of one of the two primes of Z over p, (ii) p is inert in Z with r even and $\pi = p^{r/2}\zeta$ for an imaginary quadratic root of unity $\zeta \neq \pm 1$ such that p is inert in $\mathbb{Q}(\zeta)$, or (iii) p is ramified in Z and π generates the rth power of the unique prime of Z over p. Cases (ii) and (iii) are exactly the supersingular cases, and since $D = Z$ in theses cases, the geometric endomorphism algebra is not entirely defined over κ. Hence, part (1) of Corollary 1.6.2.2 gives *all* supersingular elliptic curves over κ (up to isogeny) whose geometric endomorphism algebra is defined over κ.

By passing to products and using Theorem 1.3.4, we obtain the following result.

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

1.6.3. Example. As an application of Corollary 1.6.2.2, here are examples of simple abelian surfaces A over prime fields of any characteristic $p \not\equiv 1 \pmod{12}$ such that A is not absolutely simple. Let κ be a finite field of size p^2, with p a prime such that $p \not\equiv 1 \pmod 4$ (resp. $p \not\equiv 1 \pmod 3$). Choose ζ such that $\zeta^2 + 1 = 0$ (resp. $\zeta^2 + \zeta + 1 = 0$), so $Z := \mathbb{Q}(\zeta)$ is an imaginary quadratic field of class number

1 in which p is not split. Let $\pi = \pm p\zeta$ when p is inert in Z, and let π generate the unique prime over p in Z when p is ramified in Z, so π is a Weil p^2-integer and $Z = \mathbb{Q}(\pi)$. (Note that $\pi \neq \pm 2\sqrt{-1} = (1 \pm \sqrt{-1})^2$ since 2 is ramified in $\mathbb{Q}(\sqrt{-1})$.)

By Corollary 1.6.2.2(3) (also see Example 1.6.2.4), a simple abelian variety E_0 over κ with p^2-Frobenius equal to π must have endomorphism algebra Z and dimension 1. The elliptic curve E_0 is supersingular because p is not split in Z. The isogeny class of E_0 contains no member that is the scalar extension of an elliptic curve over $\mathbb{F}_p$, as otherwise π would have a square root $\pi_0 \in Z$, which is visibly absurd by inspection since $\pi \neq \pm 2\sqrt{-1}$.

The abelian surface $A_0 := \mathrm{Res}_{\kappa/\mathbb{F}_p}(E_0)$ satisfies $(A_0)_\kappa \simeq E_0 \times E_0^{(p)}$, so $(A_0)_\kappa$ is not simple. But A_0 is simple, as otherwise there would be a non-zero homomorphism $E_0' \to A_0$ from an elliptic curve E_0' over $\mathbb{F}_p$ and hence (by the universal property of Weil restriction) a non-zero homomorphism $(E_0')_\kappa \to E_0$, contrary to what we just saw concerning the isogeny class of E_0. (Note that $(A_0)_\kappa$ is isotypic, since $E_0^{(p)}$ is isogenous to E_0 via the relative Frobenius morphism $E_0 \to E_0^{(p)}$.)

Taking $K/\mathbb{Q}$ to be a quadratic field in which p is inert, we can lift E_0 over $\mathcal{O}_{K,(p)}$ to get an elliptic curve E over K having good reduction E_0 at $p\mathcal{O}_K$. Then $A := \mathrm{Res}_{K/\mathbb{Q}}(E)$ is an abelian surface over $\mathbb{Q}$ having good reduction $\mathrm{Res}_{\kappa/\mathbb{F}_p}(E_0)$ at p that is simple over $\mathbb{F}_p$, so (via consideration of Néron models over $\mathbb{Z}_{(p)}$) A is simple over $\mathbb{Q}$. However, $A_K \simeq E \times E'$ where E' is the twist $\sigma^*(E)$ by the non-trivial automorphism σ of K over $\mathbb{Q}$, so A_K is not simple.

1.6.4. Example. Pushing the end of Example 1.6.3 further over $\mathbb{Q}$, we now prove that if $\pi = \pm p\zeta$ and $p \equiv -1 \pmod 4$ with $\zeta^2 + 1 = 0$ (resp. $p \equiv -1 \pmod 3$ with $\zeta^2 + \zeta + 1 = 0$) then E and E' over K are not isogenous (so A_K is *not* isotypic, in contrast with its reduction $(A_0)_\kappa$). Suppose that there were an isogeny $\psi : E \to E'$, and choose it with minimal degree. In particular, ψ is not divisible by $[p]_E$. We claim that $\mathrm{ord}_p(\deg \psi)$ is odd (and in particular, is positive). Suppose otherwise, so $\deg \psi = mp^{2n}$ with $n \geqslant 0$ and $p \nmid m$. Consider the reduction $\psi_0 : E_0 \to E_0^{(p)}$ of ψ, also an isogeny with degree mp^{2n}. In particular, $\ker(\psi_0)$ is a finite subgroup scheme of E_0 with order mp^{2n}, so its p-part has order p^{2n}. But E_0 is supersingular, so it has a unique subgroup scheme of each p-power order. Hence, the p-part of $\ker(\psi_0)$ is $E_0[p^n]$, so $\psi_0 = \psi_0' \circ [p^n]_{E_0}$ with $\psi_0' : E_0 \to E_0^{(p)}$ of degree m.

Consider the composite isogeny

$$E_0 \stackrel{\psi_0'}{\to} E_0^{(p)} \to E_0^{(p^2)} = E_0$$

using the Frobenius isogeny of $E_0^{(p)}$. This is an endomorphism of E_0 with degree pm. Since $\mathrm{End}(E_0)$ is an order in $\mathbb{Z}[\zeta]$ on which the degree is computed as the norm to $\mathbb{Z}$, we get an element of $\mathbb{Z}[\zeta]$ whose norm in $\mathbb{Z}$ is divisible exactly once by p. That is impossible since p is prime in $\mathbb{Z}[\zeta]$, and so completes the verification that $\deg \psi$ has p-part p^j for some odd j.

We conclude that the finite K-subgroup $N := \ker(\psi) \subset E$ has non-trivial p-part, and this p-part has cyclic geometric fiber (as otherwise it would contain $E[p]$, contradicting that we arranged ψ to not be divisible by $[p]_E$). By cyclicity, $N[p]$ is a K-subgroup of E with order p. Consider its scheme-theoretic closure G in the Néron model of E at $p\mathcal{O}_{K,(p)}$. This is a finite flat group scheme over $\mathcal{O}_{K,(p)}$ of order p, and its special fiber G_κ is an order-p subgroup scheme of the supersingular elliptic curve E, so $G_\kappa \simeq \alpha_p$ as κ-groups (since G_κ is local-local of order p, so $\mathrm{M}^*(G_\kappa) = \kappa$ with $\mathcal{F} = \mathcal{V} = 0$). But $\mathcal{O}_{K,(p)}$ is an absolutely unramified discrete valuation ring, so there are no finite flat group schemes over $\mathcal{O}_{K,(p)}$ with special fiber α_p (by the classification results in [**123**]). This contradiction shows that E and E' are not isogenous (so A_K is not isotypic), as claimed. In fact, we have proved something stronger: if K_p denotes the p-adic completion of K then A_{K_p} is not isotypic.

1.6.5. CM lifting after a field extension and isogeny. The proof of the surjectivity aspect of the Honda-Tate theorem requires constructing abelian varieties having prescribed properties over finite fields. The idea is to relate simple abelian varieties over finite fields to simple factors of reductions of CM abelian varieties over number fields, at least after some finite extension on the initial finite field. (See [**50**] or [**121**, Lemme 3] for details.)

One can ask (as Honda implicitly did at the end of [**50**, §2]) to do better by arranging simplicity to hold for the reduction of a CM abelian variety over a number field (thereby eliminating the need to pass to a simple factor). Building on earlier work of Honda, such an improved lifting theorem was proved by Tate [**121**, Thm. 2] (and is really the starting point for the many lifting questions about CM abelian varieties that we consider in this book):

1.6.5.1. Theorem (Honda, Tate)**.** *For any isotypic abelian variety A over a finite field κ, there is a finite extension κ'/κ such that $A_{\kappa'}$ is isogenous to the reduction of a* CM *abelian variety with good reduction over a p-adic field with residue field κ'.*

Proof. By Corollary 1.6.2.5, there is a CM field $L \subset \mathrm{End}^0(A)$ with $[L:\mathbb{Q}] = 2\dim(A)$. The field L is its own centralizer in $\mathrm{End}^0(A)$, so it contains an element π which acts by the q-Frobenius endomorphism on A, where $q = \#\kappa$. Let $g = \dim(A)$. Since A is κ-isotypic, Tate's work on isogenies among abelian varieties over finite fields [**118**] gives two results for A: (i) the common characteristic polynomial over $\mathbb{Q}$ for the action of π on the Tate modules of A is a power of an irreducible polynomial f_π over $\mathbb{Q}$ (necessarily the minimal polynomial of π over $\mathbb{Q}$), and (ii) A is κ-isogenous to any g-dimensional isotypic abelian variety over κ whose q-Frobenius is a zero of f_π. Moreover, these properties persist after replacing κ with any finite extension κ' (and replacing π with $\pi^{[\kappa':\kappa]}$), due to Proposition 1.2.6.1.

By [**121**, §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 $K \subset \overline{\mathbb{Q}}_p$, a g-dimensional abelian variety B over K with good reduction at the induced p-adic place v of K, an embedding of finite fields $\kappa \hookrightarrow \kappa_v$, and an action of $\mathcal{O}_L$ on B such that the reduction B_0 at v has q_v-Frobenius in $\mathcal{O}_L$ given by the action of $\pi_v = \pi^{[\kappa_v:\kappa]} \in \mathcal{O}_L$. (Here, $q_v = \#\kappa_v$.) Since B_0 admits a CM structure over κ_v by a *field* (namely, L), it is κ_v-isotypic. Thus, since $\dim(B_0) = \dim(B)$ and A_{κ_v} satisfies $\mathrm{Fr}_{A_{\kappa_v},q_v} = \mathrm{Fr}_{A,q}^{[\kappa_v:\kappa]} = \pi_v$, it follows from the results (i) and (ii) in [**118**] recalled above that there exists a κ_v-isogeny $\phi : B_0 \to A_{\kappa_v}$. □

1.6.5.2. Remark. The κ_v-isogeny $\phi : B_0 \to A_{\kappa_v}$ at the end of the proof of Theorem 1.6.5.1 might not be L-linear, though it is $\mathbb{Q}(\pi_v)$-linear since it is compatible with q_v-Frobenius endomorphisms. We can exploit the $\mathbb{Q}(\pi_v)$-linearity of ϕ to find an L-linear κ_v-isogeny $B_0 \to A_{\kappa_v}$ as follows.

Since the q_v-Frobenius generates the center of the endomorphism algebra of any abelian variety over κ_v, the Skolem-Noether theorem ensures that any two $\mathbb{Q}(\pi_v)$-embeddings of L into the central simple $\mathbb{Q}(\pi_v)$-algebra $\mathrm{End}^0(A_{\kappa_v})$ are related through conjugation by a unit. Hence, there is an isogeny $u \in \mathrm{End}(A_{\kappa_v})$ such that $u \circ \phi$ is L-linear. By renaming this as ϕ, we may arrange that ϕ is L-linear. Thus, in Theorem 1.6.5.1 we may choose the CM lift so that the action of a *specified* degree-$2g$ CM field $L \subset \mathrm{End}^0(A)$ also lifts.

It is natural to ask for a strengthening of Theorem 1.6.5.1 in which the isogeny is applied prior to making a residue field extension (to acquire a CM lifting). As we will record near the end of 1.8, such a stronger form is true and follows from one of the main results proved later in this book.

1.7. A theorem of Grothendieck and a construction of Serre

1.7.1. Isogenies and fields of definition. Let A be an abelian variety over a field K and let $K_1 \subset K$ be a subfield. We say that A *is defined over* K_1 if there exists an abelian variety A_1 over K_1 and an isomorphism $f : A \simeq (A_1)_K$. We use similar terminology for a map $h : A \to B$ between abelian varieties over K (i.e., there exists a map $h_1 : A_1 \to B_1$ between abelian varieties over K_1 such that $(h_1)_K$ is identified with h).

For example, suppose K/K_1 is a primary extension of fields (i.e., K_1 is separably algebraically closed in K) and consider abelian varieties A and A' over K such that there are isomorphisms $f : A \simeq (A_1)_K$ and $f' : A' \simeq (A'_1)_K$ for abelian varieties A_1 and A'_1 over K_1. By Lemma 1.2.1.2, the pairs (A_1, f) and (A'_1, f') are unique up to unique isomorphism and every map $A \to A'$ as abelian varieties over K is defined over K_1 in the sense that it uniquely descends to a map $A_1 \to A'_1$ as abelian varieties over K_1. Likewise, by Corollary 1.2.1.4, all abelian subvarieties of A are defined over K_1 (and even uniquely arise from abelian subvarieties of A_1). For general extensions K/K_1 such K_1-descents may not exist, and when (A_1, f) does exist it is not necessarily unique (up to isomorphism).

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

1.7.1.2. Example. When $\mathrm{char}(K) = p > 0$, the naive analogue of Example 1.7.1.1 fails. An interesting counterexample is $A = E^2$ for a supersingular elliptic curve E over a field K of characteristic $p > 0$. The kernel H of the Frobenius isogeny $E \to E^{(p)}$ is a local-local K-group of order p, and it is the unique infinitesimal subgroup of E with order p (as any commutative infinitesimal K-group of order p has vanishing Frobenius morphism).

The only local-local finite commutative group scheme of order p over K is α_p. For perfect K this is easily proved by a computation with Dieudonné modules (as we noted in Example 1.6.4). In Proposition 3.1.10 we will prove that this property in general descends from the perfect closure (set $r = 1$ there).

Fix a choice of K-subgroup inclusion $\alpha_p \hookrightarrow E$ over K, so we get a canonical copy of α_p^2 in $A = E^2$ (as the kernel of the Frobenius isogeny $A \to A^{(p)}$). Over an arbitrary field of characteristic $p > 0$ the Frobenius and Verschiebung morphisms of α_p^2 vanish, so over any such field the non-trivial proper subgroups of α_p^2 are naturally parameterized by lines in the 2-dimensional tangent space $\mathrm{Lie}(\alpha_p^2)$; this parameterization is given by the tangent line of the subgroup (see [**23**, Thm. 3.18] for more details). In particular, the non-trivial proper K-subgroups of α_p^2 are parameterized by $\mathbb{P}^1(K)$, and if K'/K is an extension field then the non-trivial proper K'-subgroups of $(\alpha_p)^2_{K'}$ are parameterized by $\mathbb{P}^1(K')$ (with the subset $\mathbb{P}^1(K)$ consisting of the tangent lines to the K'-subgroups defined over K).

We conclude that if K'/K is a non-trivial extension field then there are K'-subgroups $G' \subset A' := A_{K'}$ of order p that are contained in $(\alpha_p^2)_{K'}$ and do not arise from a K-subgroup of A. In contrast with what we saw in Example 1.7.1.1 for isogeny classes over algebraically closed fields of characteristic 0, we claim that if K is separably closed (or more generally if K is separably closed in K', with G' not defined over K inside $A' = A_{K'}$) then the isogenous quotient A'/G' of $A' = A_{K'}$ cannot be defined over K as an abstract abelian variety!

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

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

descends to an isogeny $A \to B$ over K by Lemma 1.2.1.2 (since K'/K is primary). The kernel of this latter isogeny is a K-subgroup of A that descends $G' \subset A'$, contrary to how G' was chosen. Thus, no such B exists.

One lesson we learn from Example 1.7.1.1 and Example 1.7.1.2 is that fields of definition for abelian varieties in positive characteristic are rather more subtle than in characteristic 0, even when working over algebraically closed base fields.

1.7.2. Grothendieck's theorem. To fully appreciate the significance of Example 1.7.1.2, we turn our attention to a striking result of Grothendieck concerning the field of definition of an abelian variety with sufficiently many complex multiplications in positive characteristic. Before stating Grothendieck's result, we record the analogue in characteristic 0 that is a source of inspiration.

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

Proof. By Example 1.7.1.1, without loss of generality we may replace A with an isogenous abelian variety. Thus, by Proposition 1.3.2.1 we can pass to the isotypic (and even simple) case, and so by Theorem 1.3.4 the abelian variety A over K admits complex multiplication by a CM field L. Let Φ be the resulting CM type on L. Letting $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in K, we may view Φ as a $\overline{\mathbb{Q}}$-valued CM type on L.

By Proposition 1.5.4.1 (applied over the algebraically closed base field $\overline{\mathbb{Q}}$) there is a CM abelian variety B over $\overline{\mathbb{Q}}$ with complex multiplication by L and CM type Φ (viewed as valued in $\overline{\mathbb{Q}}$). The abelian variety B_K over K admits complex multiplication by L with associated CM type Φ (viewed as valued in K), so by applying Proposition 1.5.4.1 over K we see that B_K is L-linearly isogenous to A over K (as these two abelian varieties over K are endowed with complex multiplication by L yielding the same CM type Φ on L). Fix such an isogeny $f : B_K \to A$. By Example 1.7.1.1 (applied to $K/\overline{\mathbb{Q}}$), the finite kernel of f descends to a finite subgroup of B. The quotient of B by this descent of $\ker(f)$ is a descent A_0 of $A = B_K/\ker(f)$ to an abelian variety over $\overline{\mathbb{Q}}$.

By Lemma 1.2.1.2, $\mathrm{End}(A_0) \to \mathrm{End}(A)$ is an isomorphism. Thus, we may assume the base field K is an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Express $\overline{\mathbb{Q}}$ as a direct limit of number fields to see that the $\overline{\mathbb{Q}}$-group A descends to an abelian variety over a number field inside $\overline{\mathbb{Q}}$. The same direct limit argument as used at the start of the proof of Proposition 1.2.6.1 then shows that we can choose the descent of A to a number field so that all elements of $\mathrm{End}(A)$ descend as well. □

Theorem 1.7.2.1 can be formulated with a general ground field K of characteristic 0, but the nature of the descent becomes a bit more subtle. Namely, if A is an abelian variety over a field K of characteristic 0 and if A admits sufficiently many complex multiplications, then there is a finite extension K'/K such that $A_{K'}$ descends (along with its entire endomorphism algebra) to an abelian variety over a number field contained in K'. In this formulation it is crucial to introduce the finite extension K'/K, even if we just wish to descend the abelian variety (and not any specific endomorphisms). This is illustrated by quadratic twists of elliptic curves:

1.7.2.2. Example. Consider a CM elliptic curve over $\mathbb{C}$ and extend scalars to $K = \mathbb{C}(t)$. Let E be the quadratic twist of this scalar extension by a quadratic extension K'/K, so E is a CM elliptic curve over K whose ℓ-adic representation for $\mathrm{Gal}(K_s/K)$ is non-trivial. No member of the isogeny class of E over K can be defined over $\mathbb{C}$ (let alone over $\overline{\mathbb{Q}}$), as all members of the isogeny class have non-trivial action by $\mathrm{Gal}(K_s/K)$ for their ℓ-adic representations. Of course, if we pass up to $\overline{K}$ then the effect of quadratic twisting goes away and there is no obstruction to descent to $\overline{\mathbb{Q}}$.

Over number fields, CM abelian varieties extend to abelian schemes over the entire ring of integers at the cost of a finite extension of the ground field. This is an application of the semi-stable reduction theorem for abelian varieties (see [**109**, Thm. 6]), and we record it here for later reference:

1.7.2.3. Theorem. *Every* CM *abelian variety over a number field has potentially good reduction at all places.*

Since every abelian variety over an algebraic closure of $\mathbb{F}_p$ descends to a finite field and hence has sufficiently many complex multiplications (by Corollary 1.6.2.5), a first guess for an analogue of Theorem 1.7.2.1 in positive characteristic is that CM abelian varieties over algebraically closed fields K with positive characteristic can be descended to the algebraic closure of the prime field inside K (or equivalently, to a finite subfield of K).

Example 1.7.1.2 shows that this guess is false, since A'/G' as built there admits a CM structure since supersingular elliptic curves over K always admit a CM structure (as they descend to elliptic curves over the algebraic closure of $\mathbb{F}_p$ inside K). Allowing isogenies does not eliminate the need for a finite extension when the ground field K is not algebraically closed:

1.7.2.4. Example. For a finite field κ, Example 1.7.2.2 adapts to work over $K = \kappa(t)$ by beginning with an elliptic curve over κ (for which complex multiplication by an imaginary quadratic field exists in general; see Corollary 1.6.2.5). One can do likewise over $\kappa(t)$ with κ an algebraic closure of $\mathbb{F}_p$.

Motivated by the above examples, Grothendieck proved a reasonable analogue of Theorem 1.7.2.1 in positive characteristic:

1.7.2.5. Theorem (Grothendieck)**.** *Let A be an abelian variety over a field K with $\mathrm{char}(K) = p > 0$, and assume A admits sufficiently many complex multiplications. Then there exists a finite extension K' of K, a finite subfield $\kappa \subset K'$, and an abelian variety B over κ such that the scalar extensions $A \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K')$ and $B \times_{\mathrm{Spec}(\kappa)} \mathrm{Spec}(K')$ over K' are isogenous.* □

For an exposition of Grothendieck's proof, see [**89**]. The essential difficulty in the proof in contrast with characteristic 0 is that the isogeny cannot be avoided, even when $K = \overline{K}$ (due to Example 1.7.1.2). The proof of Theorem 1.7.2.5 is immediately reduced to the case when K is finitely generated over $\mathbb{F}_p$. Grothendieck used the theory of potentially good reduction to find the required K'/K and made a descent from K' to a finite subfield via a Chow trace (in the sense of [**23**, §6]).

1.7.3. There is a refinement of Grothendieck's theorem, due to C-F. Yu, that clarifies the role of the isogeny and proceeds in a simpler way by using moduli spaces of abelian varieties. This refinement is given in 1.7.5. We will not need that result, but the main ingredient in its proof is a technique to modify the endomorphism ring that will be very useful later, so we now explain that technique.

As motivation, consider an abelian variety A of dimension $g > 0$ over a field K such that A admits sufficiently many complex multiplications, and let $P \subset \mathrm{End}^0(A)$ be a commutative semisimple $\mathbb{Q}$-subalgebra with $[P : \mathbb{Q}] = 2g$. The intersection $\mathcal{O} := P \cap \mathrm{End}(A)$ is an order in P that may not be maximal (i.e., it may not equal $\mathcal{O}_P := \prod \mathcal{O}_{L_i}$, where $\prod L_i$ is the decomposition of P into a finite product of number fields). It is natural to ask if there is an isogenous abelian variety for which the non-maximality problem goes away. The following discussion addresses this issue.

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

We need an algebraic variant of the analytic construction in Example 1.7.3.1. Observe that $\mathcal{O}_P \cdot \Lambda$ is the image of the natural map $\mathcal{O}_P \otimes_{\mathcal{O}} \Lambda \to V$. Inspired by this, we are led to ask if these is a way to enlarge an endomorphism ring via a "tensor product" against a finite-index extension of coefficient rings. There is a construction of this sort due to Serre [**104**], applicable over any base scheme, though it turns out to not be applicable to the above situation because $\mathcal{O}_P$ is not a projective $\mathcal{O}$-module when $\mathcal{O} \neq \mathcal{O}_P$. We wish to adapt Serre's construction to the above situation over a field, so we digress to explain Serre's procedure.

1.7.4. Serre's tensor construction. Consider a scheme S, a commutative ring $\mathcal{O}$, and an $\mathcal{O}$-module scheme A over S. (The main example of such an A to keep in mind is an abelian scheme, but there are other interesting examples, such the n-torsion subgroups of such abelian schemes for $n \geqslant 1$.) Let M be a projective $\mathcal{O}$-module of finite rank.

The projectivity of M ensures that the functor $T \rightsquigarrow M \otimes_{\mathcal{O}} A(T)$ on S-schemes is represented by an S-scheme, denoted $M \otimes_{\mathcal{O}} A$, and that $M \otimes_{\mathcal{O}} A$ inherits many nice properties from A such as flatness, smoothness, properness, good behavior with respect to analytification over $\mathbb{C}$, etc. The interested reader can see [**22**, §7] for details (where non-commutative $\mathcal{O}$ are also considered), but the idea of the construction of $M \otimes_{\mathcal{O}} A$ is simple, as follows.

If $\mathcal{O}^r \overset{\varphi}{\to} \mathcal{O}^s \to M \to 0$ is a presentation then we want to define $M \otimes_{\mathcal{O}} A$ to be the cokernel of the S-group map $A^r \to A^s$ induced by the matrix of φ. Without the projectivity assumption on the $\mathcal{O}$-module M, over a general base scheme S such a quotient may not exist. However, since M is locally free of finite rank as an $\mathcal{O}$-module (by the projectivity hypothesis) we can instead begin with a presentation of the dual module $M^\vee$ and then dualize to get a left-exact sequence $0 \to M \to \mathcal{O}^s \to \mathcal{O}^r$ with suitable local splitting properties to enable us to construct $M \otimes_{\mathcal{O}} A$ as a scheme-theoretic kernel. More explicitly, by projectivity there is an integer $r \geqslant 1$ and $\mathcal{O}$-module M' such that $\mathcal{O}^r \simeq M \oplus M'$, so there is an $\mathcal{O}$-linear idempotent endomorphism e of $\mathcal{O}^r$ such that $M = \ker(e)$. The kernel of the associated $\mathcal{O}$-linear endomorphism of A^r represents $M \otimes_{\mathcal{O}} A$.

1.7.4.1. Example. Let L be a CM field, and let (A, i) and (A', i') be CM abelian varieties over a field K, where i and i' respectively define complex multiplication by L. Assume that via these embeddings, $\mathcal{O}_L$ lies in the endomorphism rings of the abelian varieties. Finally, assume that there exists a non-zero $\mathcal{O}_L$-linear map $A' \to A$. (By Proposition 1.5.4.1, when K is algebraically closed of characteristic 0 it is equivalent to assume that the associated CM types Φ' and Φ on L coincide.)

We claim that $M := \mathrm{Hom}((A', i'), (A, i))$ is an invertible $\mathcal{O}_L$-module whose formation is unaffected by extension of the ground field and that if $\mathrm{char}(K) = 0$ then the evaluation map

$$M \otimes_{\mathcal{O}_L} A' \to A$$

is an isomorphism. (Hence, over an algebraically closed field of characteristic 0 the Serre tensor construction defines a natural *transitive* action of the finite group $\mathrm{Pic}(\mathcal{O}_L)$ on the set of isomorphism classes of CM abelian varieties with a fixed CM type (L, Φ) and CM order $\mathcal{O}_L$. The argument below will show that the action is simply transitive.)

The non-zero L-vector space $M_{\mathbb{Q}} = \mathrm{Hom}^0((A', i'), (A, i))$ has dimension exactly 1 since for $\ell \neq \mathrm{char}(K)$ the natural map

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} M_{\mathbb{Q}} \to \mathrm{Hom}_{L_\ell}(V_\ell(A'), V_\ell(A))$$

is injective and the target is free of rank 1 over L_ℓ. Hence, the finitely generated torsion-free $\mathcal{O}_L$-module M is invertible. Also, the injective map

$$\mathrm{Hom}((A', i'), (A, i)) \to \mathrm{Hom}((A'_{K_s}, i'), (A_{K_s}, i))$$

between finitely generated $\mathcal{O}_L$-modules has image with finite index since it becomes an equality after applying $\mathbb{Q} \otimes_{\mathbb{Z}} (\cdot)$ (for L-dimension reasons); let n be the index. It follows that all L-linear K_s-homomorphisms $f : A'_{K_s} \to A_{K_s}$ are $\mathrm{Gal}(K_s/K)$-invariant because nf is defined over K. This shows that the formation of M is unaffected by ground field extension to K_s, and hence by any ground field extension (due to Lemma 1.2.1.2).

Now we assume that $\mathrm{char}(K) = 0$ and seek to prove that $M \otimes_{\mathcal{O}_L} A' \to A$ is an isomorphism. We may assume K is finitely generated, and then that $K = \mathbb{C}$. The $\mathcal{O}_L$-modules $\mathrm{H}_1(A(\mathbb{C}), \mathbb{Z})$ and $\mathrm{H}_1(A'(\mathbb{C}), \mathbb{Z})$ are each invertible (due to being $\mathbb{Z}$-flat of rank $[L : \mathbb{Q}]$). By Example 1.5.3, we get $\mathcal{O}_L$-linear isomorphisms $A(\mathbb{C}) = (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi/\mathfrak{a}$ and $A'(\mathbb{C}) = (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi/\mathfrak{a}'$ for non-zero ideals $\mathfrak{a}, \mathfrak{a}' \subset \mathcal{O}_L$. Hence, elements of M are precisely multiplication on $(\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi$ by those $c \in L$ such that $c\mathfrak{a}' \subseteq \mathfrak{a}$. We conclude that $M = \mathrm{Hom}_{\mathcal{O}_L}(\mathfrak{a}', \mathfrak{a}) = \mathfrak{a}{\mathfrak{a}'}^{-1}$, with $M \otimes_{\mathcal{O}_L} A' \to A$ given by the evident evaluation pairing on $\mathbb{C}$-points. This is an isomorphism because the induced map on homology lattices is the natural map $M \otimes_{\mathcal{O}_L} \mathfrak{a}' \to \mathfrak{a}$ that is clearly an isomorphism.

The isomorphism property for the map $M \otimes_{\mathcal{O}_L} A' \to A$ in Example 1.7.4.1 fails away from characteristic 0, even for elliptic curves over finite fields. For example, if L is imaginary quadratic with class number 1 then the relative Frobenius isogeny provides counterexamples (using elliptic curves whose j-invariant is not in the prime field). More explicitly, for $p \equiv -1 \bmod 4$ and $\kappa := \mathbb{Z}[i]/(p) \simeq \mathbb{F}_{p^2}$ with $p > 3$, consider the elliptic curves $E_\pm = E = \{y^2 = x^3 - x\}$ over κ with CM by $\mathcal{O}_L$ via the actions $[i](x, y) = (-x, \pm iy)$. These are not $\mathcal{O}_L$-linearly isomorphic (since $\mathrm{Aut}(E) = \mu_4 \subset \mathcal{O}_L^\times$, as $p > 3$) but the Frobenius isogeny $E \to E^{(p)}$ is an $\mathcal{O}_L$-linear isogeny $E_+ \to E_-$. Thus, the module M of $\mathcal{O}_L$-linear homomorphisms from E_+ to E_- is non-zero but the $\mathcal{O}_L$-linear map $M \otimes_{\mathcal{O}_L} E_+ \to E_-$ cannot be an isomorphism (since $M \simeq \mathcal{O}_L$ as $\mathcal{O}_L$-modules).

1.7.4.2. Example. Let (A, i, L) be as in Example 1.7.4.1 over a field K, so $\mathcal{O}_L \subset \mathrm{End}(A)$. For an invertible $\mathcal{O}_L$-module M, another such abelian variety is given by $M \otimes_{\mathcal{O}_L} A$. Any $m \in M$ defines an $\mathcal{O}_L$-linear map $e_m : A \to M \otimes_{\mathcal{O}_L} A$ via $x \mapsto m \otimes x$. For $\ell \neq \mathrm{char}(K)$, the map $T_\ell(e_m)$ induced by e_m on ℓ-adic Tate modules is the map $T_\ell(A) \to M \otimes_{\mathcal{O}_L} T_\ell(A)$ given by $v \mapsto m \otimes v$, so $e_m \neq 0$ when $m \neq 0$. In particular, the module $\mathrm{Hom}_{\mathcal{O}_L}(A, M \otimes_{\mathcal{O}_L} A)$ of $\mathcal{O}_L$-linear homomorphisms is non-zero and therefore invertible (by Example 1.7.4.1).

The natural map of invertible $\mathcal{O}_L$-modules

$$e_{A,M} : M \to \mathrm{Hom}_{\mathcal{O}_L}(A, M \otimes_{\mathcal{O}_L} A)$$

is injective, hence of finite index. We shall now show that this map is an isomorphism. It suffices to check the result after applying $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} (\cdot)$ for *every* prime ℓ (allowing $\ell = \mathrm{char}(K)$). This scalar extension is the first map in the diagram

$$M_\ell \to \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathcal{O}_L}(A, M \otimes_{\mathcal{O}_L} A) \to \mathrm{Hom}_{\mathcal{O}_{L,\ell}}(A[\ell^\infty], M_\ell \otimes_{\mathcal{O}_{L,\ell}} A[\ell^\infty])$$

whose second map is injective (Proposition 1.2.5.1) and composition is the canonical homomorphism that is injective. It therefore suffices to show that the composite map is an isomorphism. But M_ℓ is free of rank 1 as an $\mathcal{O}_{L,\ell}$-module, so it is equivalent to show that the natural map

$$\mathcal{O}_{L,\ell} \to \mathrm{End}_{\mathcal{O}_{L,\ell}}(A[\ell^\infty])$$

is an isomorphism for all ℓ.

The case $\ell \neq \mathrm{char}(K)$ is trivial, as then the ℓ-adic Tate module $T_\ell(A)$ is free of rank 1 over $\mathcal{O}_{L,\ell}$ (since $V_\ell(A)$ is free of rank 1 over L_ℓ, due to faithfulness and $\mathbb{Q}_\ell$-dimension reasons). Now assume $\mathrm{char}(K) = p > 0$ and $\ell = p$. Decomposing $A[p^\infty]$ according to the primitive idempotents of $\mathcal{O}_{L,p}$, for each p-adic place v of L the v-factor has height at least $[L_v : \mathbb{Q}_p]$ (by Proposition 1.4.3.9) and hence height exactly $[L_v : \mathbb{Q}_p]$. Thus, it suffices to prove more generally that if X is a p-divisible group over K of height $h > 0$ and F is a p-adic field of degree h over $\mathbb{Q}_p$ such that $\mathcal{O}_F \subset \mathrm{End}(X)$ then $\mathcal{O}_F$ is its own centralizer in $\mathrm{End}(X)$.

We may and do assume that K is algebraically closed, so the Dieudonné module $\mathrm{M}^*(X)$ makes sense and is free of rank 1 as a $W(K) \otimes_{\mathbb{Z}_p} \mathcal{O}_F$-module (Proposition 1.4.3.9). Thus, any $\mathcal{O}_F$-linear endomorphism f of X gives rise to a $W(K) \otimes_{\mathbb{Z}_p} \mathcal{O}_F$-linear endomorphism of $\mathrm{M}^*(X)$, so $\mathrm{M}^*(f)$ must be multiplication by some $c \in W(K) \otimes_{\mathbb{Z}_p} \mathcal{O}_F$. But $\mathrm{M}^*(f)$ commutes with the $\mathcal{F}$ operator on $\mathrm{M}^*(X)$, so c is invariant under the absolute Frobenius automorphism σ of $W(K)$. This forces $c \in W(K)^{\sigma=1} \otimes_{\mathbb{Z}_p} \mathcal{O}_F = \mathcal{O}_F$, so f is an $\mathcal{O}_F$-multiplier, as desired.

1.7.4.3. Remark. The $\mathcal{O}$-linear projectivity hypothesis on M in the construction of $M \otimes_{\mathcal{O}} A$ cannot be dropped, even when the base is the spectrum of a discrete valuation ring. For example, if R is a p-adic discrete valuation ring and E is an elliptic curve over R with endomorphism ring $\mathcal{O} = \mathbb{Z}[p\sqrt{-p}]$ (as can be easily constructed using classical CM theory for elliptic curves), then for the non-projective $\mathcal{O}$-module $M = \mathbb{Z}[\sqrt{-p}]$ the fppf sheafification of the functor $T \rightsquigarrow M \otimes_{\mathcal{O}} E(T)$ on R-schemes is not representable. (The idea is as follows. First one proves that a representing object, if one exists, must be an elliptic curve $\mathscr{E}$. By presenting M over $\mathcal{O}$ using two generators and two relations, we get a quotient homomorphism $E \times E \to \mathscr{E}$ whose kernel must be an R-flat divisor in $E \times E$. Studying its defining equation in the formal group of $E \times E$ leads to a contradiction.)

For any homomorphism $f : A \to A'$ between abelian varieties over a field, the image $f(A)$ is an abelian subvariety over A' and the map $A \to f(A)$ is flat. Such good properties for $f(A)$ generally fail for homomorphisms between abelian schemes over a more general base, but their availability over fields enables us to push through the initial cokernel idea for the Serre tensor construction over fields. In this way we can avoid dualizing M and hence make the construction work with weaker hypotheses on M than projectivity. We shall now give a version of this for abelian varieties (and in 4.3.1 there is a version for p-divisible groups), but first we require a general lemma:

1.7.4.4. Lemma. *For an abelian variety B over a field K and an abelian subvariety B', the quotient sheaf B/B' for the fppf topology on the category of K-schemes is represented by an abelian variety.*

PROOF. Recall from the Poincaré reducibility theorem over K (see Theorem 1.2.1.3) that there is an abelian subvariety $B'' \subset B$ over K that is an isogeny complement to B' in the sense that the natural map $f : B' \times B'' \to B$ is an isogeny. Since f is a finite flat surjection, so $B \simeq (B' \times B'')/\ker(f)$ as fppf abelian sheaves, we likewise have $B/B' = B''/(B' \cap B'')$ as fppf sheaves. Thus, the problem for B/B' is the same as for the quotient of B'' by the finite K-subgroup scheme $B' \cap B''$. Hence, it suffices to show that B''/G is (represented by) an abelian variety for any finite K-subgroup $G \subset B''$.

Rather than appealing to existence results for quotients by the free action of a finite group scheme on a quasi-projective scheme, here is a more direct argument via fppf descent theory and a special property of abelian varieties: for any $n \geqslant 1$, the map $[n]_{B''} : B'' \to B''$ is a finite flat surjection, so $B''/B''[n] \simeq B''$ as fppf abelian sheaves. To exploit this, note that the K-group G is killed by its order n. (Indeed, we may assume $\mathrm{char}(K) = p > 0$ and use the connected-étale sequence for G and kernels of relative Frobenius morphisms to reduce to the case when $\mathrm{Fr}_{G/K}$ vanishes. In such cases p kills G since $[p]_G = \mathrm{Ver}_{G^{(p)}/K} \circ \mathrm{Fr}_{G/K}$.) Thus, $G \subset B''[n]$, so as fppf abelian sheaves B''/G is a $B''[n]/G$-torsor over $B''/B''[n] \simeq B''$.

Since $B''[n]/G$ is represented by a finite K-scheme, by effective descent for finite morphisms we see that the quotient sheaf B''/G is therefore represented by a finite flat B''-scheme over which B'' is a finite flat cover (even a G-torsor). This implies that B''/G is proper, smooth, and connected, so it is an abelian variety, as desired. $\square$

Here is the promised generalized Serre tensor construction over fields (allowing non-projective modules).

1.7.4.5. Proposition. *Let A be an abelian variety or finite commutative group scheme over a field K. Let $\mathcal{O} \to \mathrm{End}(A)$ be a homomorphism from a commutative ring. For any finitely generated $\mathcal{O}$-module M, the functor $T \rightsquigarrow M \otimes_{\mathcal{O}} A(T)$ on K-schemes has fppf sheafification that is respectively represented by an abelian variety or finite commutative group scheme $M \otimes_{\mathcal{O}} A$.*

Suppose A is an abelian variety. For an injective map $M \to N$ between torsion-free $\mathcal{O}$-modules with finite cokernel, the induced map $M \otimes_{\mathcal{O}} A \to N \otimes_{\mathcal{O}} A$ is an isogeny. In particular, if $\mathcal{O}'$ is a $\mathbb{Z}$-flat $\mathcal{O}$-algebra that is finitely generated as an $\mathcal{O}$-module and $\mathcal{O}_{\mathbb{Q}} \to \mathcal{O}'_{\mathbb{Q}}$ is an isomorphism then the natural map of abelian varieties $A \to A' := \mathcal{O}' \otimes_{\mathcal{O}} A$ is an isogeny and the identification $\mathrm{End}^0(A) = \mathrm{End}^0(A')$ *carries $\mathcal{O}' \subset \mathrm{End}^0(A)$ into* $\mathrm{End}(A')$.

The notation $\mathcal{O}' \otimes_{\mathcal{O}} A$ should not be confused with the standard notation for affine base change of schemes. Also, if M is killed by a non-zero element of $\mathcal{O}$ then it is killed by a non-zero integer and hence the abelian variety $M \otimes_{\mathcal{O}} A$ vanishes.

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

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

The map φ is given by an $s \times r$ matrix over $\mathcal{O}$, so it defines an analogous map $[\varphi] : A^r \to A^s$ between K-groups. Since we are working over a field, if A is an abelian variety then the map $[\varphi]$ has image that is an abelian subvariety of A^s onto which $[\varphi]$ is faithfully flat. If instead A is a finite commutative K-group then there is a finite flat quotient map $A^r \to A^r/\ker[\varphi]$. The induced map $A^r/\ker[\varphi] \to A^s$

between finite K-groups has trivial kernel, so it is a closed immersion. We denote this closed K-subgroup as $[\varphi](A^r)$, so (as with abelian varieties) the map $[\varphi]$ is faithfully flat onto a closed K-subgroup $[\varphi](A^r) \subset A^s$.

Using Lemma 1.7.4.4 in the abelian variety case and the more elementary theory of quotients for finite commutative K-group schemes in the finite case, the quotient $M \otimes_{\mathcal{O}} A := A^s/[\varphi](A^r)$ as an abelian variety or finite K-group scheme represents the cokernel of $[\varphi]$ in the sense of fppf abelian sheaves on the category of K-schemes. It follows (via the right-exactness of algebraic tensor products) that the K-group scheme $M \otimes_{\mathcal{O}} A$ represents the fppf sheafification of $T \rightsquigarrow M \otimes_{\mathcal{O}} A(T)$.

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

The assertions concerning $\mathcal{O}'$ follow by considering the functor $T \rightsquigarrow \mathcal{O}' \otimes_{\mathcal{O}} A(T)$ and the abelian variety over K representing it. □

As an application of the Serre tensor construction with non-projective modules when the base is a field, we prove a precise form of the "lifting" part of the Deuring Lifting Theorem:

1.7.4.6. Theorem (Deuring). *Let E_0 be an elliptic curve over $\mathbb{F}_q$. For any $f_0 \in \mathrm{End}(E_0)$ generating an imaginary quadratic field $L \subset \mathrm{End}^0(E_0)$ and p-adic place $\mathfrak{p}$ of $\mathcal{O}_L$, let R be the valuation ring of the compositum $W(\mathbb{F}_q)[1/p] \cdot L_{\mathfrak{p}}$ over $\mathbb{Q}_p$.*

There exists a CM *elliptic curve E over R equipped with an endomorphism f such that (E, f) has special fiber isomorphic to (E_0, f_0).*

By 1.6.2.5, for any E_0 over $\mathbb{F}_q$ there is an imaginary quadratic field L inside $\mathrm{End}^0(E_0)$. The CM structure forces R to have residue field $\mathbb{F}_q$, as we shall see in the proof below.

Proof. If E_0 is ordinary then $L_{\mathfrak{p}} = \mathbb{Q}_p$ and we can choose E to be the Serre–Tate canonical lift over $W(\mathbb{F}_q)$, to which all endomorphisms of E_0 uniquely lift; see 1.4.5.4. Suppose instead that E_0 is supersingular. It suffices to show that for any imaginary quadratic field $L \subset \mathrm{End}^0(E_0)$ and $\mathcal{O} := \mathrm{End}(E_0) \bigcap \mathcal{O}_L$, we can lift (E_0, α_0) over R where $\alpha_0 : \mathcal{O} \hookrightarrow \mathrm{End}(E_0)$ is the natural inclusion.

Consider the canonical $\mathcal{O}$-linear isogeny

$$h : E_0 \to E_0' := \mathcal{O}_L \otimes_{\mathcal{O}} E_0$$

(see 1.7.4.5). The key point is to show that p does not divide the degree of h (so h induces an isomorphism on p-divisible groups). The degree of h is the order of the finite $\mathbb{F}_q$-group $\ker(h)$, so if this kernel is étale then its order must be relatively prime to p because a supersingular elliptic curve has infinitesimal p-torsion. Thus, we may assume $\ker(h)$ is not étale, so the infinitesimal identity component of $\ker(h)$ is nontrivial and therefore the relative Frobenius morphism of $\ker(h)$ has nontrivial kernel. The $\mathcal{O}$-linear relative Frobenius morphism $\mathrm{Fr}_{E_0/\mathbb{F}_q} : E_0 \to E_0^{(p)}$ for the elliptic curve E_0 has kernel of order p, so this latter kernel must lie inside $\ker(h)$.

We conclude that if $\ker(h)$ is not étale then h factors through $\mathrm{Fr}_{E_0/\mathbb{F}_q}$, so there is a commutative diagram

$$\begin{array}{ccc} E_0 & \xrightarrow{h} & \mathcal{O}_L \otimes_{\mathcal{O}} E_0 \\ {\scriptstyle \mathrm{Fr}_{E_0/\mathbb{F}_q}} \downarrow & \nearrow & \downarrow {\scriptstyle 1\otimes \mathrm{Fr}_{E_0/\mathbb{F}_q}} \\ E_0^{(p)} & \xrightarrow[h^{(p)}]{} & \mathcal{O}_L \otimes_{\mathcal{O}} E_0^{(p)} \end{array}$$

of $\mathcal{O}$-linear isogenies. Since $h^{(p)}$ is the initial $\mathcal{O}$-linear map from $E_0^{(p)}$ to an $\mathcal{O}_L$-linear module scheme over $\mathbb{F}_q$, the right vertical map must be an isomorphism. This latter map is the relative Frobenius isogeny for the elliptic curve $\mathcal{O}_L \otimes_{\mathcal{O}} E_0$, as that also makes the outside square commute (and commutativity uniquely determines the right vertical map in terms of the other maps on the outside of the diagram). The Frobenius isogeny for an elliptic curve over $\mathbb{F}_q$ is not an isomorphism, so we have a contradiction. Thus, $\ker(h)$ is étale and hence has order not divisible by p.

We conclude that h induces an isomorphism on p-divisible groups, so by the Serre–Tate deformation theorem it follows that the formal deformation theory of E_0 is the same as that of E_0'. Any formal deformation of E_0 over a complete local noetherian $W(\mathbb{F}_q)$-algebra is a scheme, since the inverse ideal sheaf of the identity section provides a canonical algebraization, so by using formal GAGA for morphisms [**34**, III_1, 5.4.1] to keep track of the CM structure we may replace E_0 with E_0' to arrange that $\mathcal{O}_L \subset \mathrm{End}(E_0)$.

The $\mathcal{O}_L$-action on $\mathrm{Lie}(E_0)$ selects a prime over p in $\mathcal{O}_L$ and embeds its residue field into $\mathbb{F}_q$. Pre-composing the $\mathcal{O}_L$-action on E_0 with the involution of L if necessary, we can arrange that $\mathcal{O}_L$ acts on $\mathrm{Lie}(E_0)$ through an embedding $\mathcal{O}_L/\mathfrak{p} \hookrightarrow \mathbb{F}_q$, so the formal group corresponding to $E_0[p^\infty]$ is a formal $\mathcal{O}_{L,\mathfrak{p}}$-module over $\mathbb{F}_q$ of dimension 1. Both Lubin–Tate theory and the deformation theory of 1-dimensional formal modules [**49**, 22.4.4] ensure that this lifts to a formal $\mathcal{O}_{L,\mathfrak{p}}$-module over R, so we obtain the desired $\mathcal{O}_L$-linear formal lift of E_0 over R. □

1.7.5. Variant on Grothendieck's theorem. C-F. Yu's variant on Theorem 1.7.2.5 asserts that we can *first* apply an isogeny and *then* pass to a finite extension on K (with no further isogeny involved) to get to a situation that descends to a finite field. This goes as follows. Consider the setup in Theorem 1.7.2.5. By Proposition 1.3.2.1, the simple factors have sufficiently many complex multiplications, so we may focus on the case of simple abelian varieties A. Choose a polarization, so the division algebra $D = \mathrm{End}^0(A)$ is endowed with a positive involution. By [**133**, 2.2], there is a maximal commutative subfield $L \subset D$ that is stable under the involution, so L is either totally real or CM. We claim that L is a CM field, or in other words L is not totally real.

To prove this property of L, first note that by Proposition 1.3.6.4 (in positive characteristic) the division algebra D is either of Type III or Type IV (in the sense of Theorem 1.3.6.2). Since L contains the center Z of D, for Type IV we get the CM property for L from the fact that Z is CM in such cases. For Type III, the key point is that Z is totally real and D is non-split at all real places of Z. We know that D_L is split over L since L is a maximal commutative subfield of D, so L is not totally real. Hence, once again L is a CM field.

Applying Proposition 1.7.4.5, we can pass to an isogenous abelian variety so that $\mathcal{O}_L \subset \mathrm{End}(A)$. In this special case, we may conclude via the following theorem.

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

This result is [**133**, Thm. 1.3]; it will not be used in what follows. (Note that it suffices just to descend the abelian variety $A_{K'}$ to a finite subfield of K', as then a further finite extension on K' will enable us to descend the abelian variety along with its $\mathcal{O}_L$-action, by Lemma 1.2.1.2.)

1.8. CM lifting questions

1.8.1. Basic definitions and examples. Let κ be a field of characteristic $p > 0$, and consider an abelian variety A_0 over κ. By Corollary 1.6.2.5, if κ is finite and A_0 is isotypic then we may endow it with a structure of CM abelian variety having complex multiplication by a CM field. Inspired in part by Theorem 1.6.5.1, we wish to pose several questions related to the problem of lifting A_0 to characteristic 0 in the presence of CM structures. First we make a general definition unrelated to complex multiplication.

1.8.1.1. Definition. A *lifting* of A_0 to characteristic 0 is a triple (R, A, ϕ) consisting of a domain R of characteristic 0, an abelian scheme A over R, a surjective map $R \twoheadrightarrow \kappa$, and an isomorphism $\phi : A_\kappa \simeq A_0$ of abelian varieties over κ.

We may replace R with its localization at the maximal ideal $\ker(R \twoheadrightarrow \kappa)$ so that R is local with residue field κ. For $K := \mathrm{Frac}(R)$, if A_K admits sufficiently many complex multiplications then we say A is a CM *lift* of A_0 to characteristic 0. The injective map $\mathrm{End}(A) \to \mathrm{End}(A_K)$ has torsion-free cokernel:

1.8.2. Lemma. *For abelian schemes A, B over an integral scheme S with generic point η, the injective map $\mathrm{Hom}(A, B) \to \mathrm{Hom}(A_\eta, B_\eta)$ has torsion-free cokernel.*

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

The injective map in Lemma 1.8.2 can fail to be surjective:

1.8.3. Example. Let p be a prime with $p \equiv 3 \pmod 4$, so p is prime in $\mathbb{Z}[i]$ (with $i^2 = -1$). Let $R = \mathbb{Z}_{(p)} + p\mathbb{Z}_{(p)}[i]$, so $[\mathbb{Z}_{(p)}[i] : R] = p$ and $\mathrm{Frac}(R) = \mathbb{Q}(i)$. Let E be the elliptic curve $y^2 = x^3 - x$ over R, so the generic fiber $E_{\mathbb{Q}(i)}$ has endomorphism ring $\mathbb{Z}[i]$ via the action $[i](x, y) = (-x, -iy)$. Because $[i]^*(\mathrm{d}x/y) = i \cdot \mathrm{d}x/y$, $\mathbb{Z}[i]$ acts on $\mathrm{Lie}(E_{\mathbb{Q}(i)})$ through scaling via the canonical inclusion $\mathbb{Z}[i] \hookrightarrow \mathbb{Q}(i)$.

We claim that $\mathrm{End}(E) = \mathbb{Z}$ (so $\mathrm{End}^0(E) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E) = \mathbb{Q}$, even though the generic fiber $E_{\mathbb{Q}(i)}$ has endomorphism algebra $\mathbb{Q}(i)$). Indeed, if not then $\mathrm{End}(E)$ is an order in $\mathbb{Z}[i] = \mathrm{End}(E_{\mathbb{Q}(i)})$, so $\mathrm{End}(E) = \mathbb{Z}[i]$ by Lemma 1.8.2. In particular, the action by i on $E_{\mathbb{Q}(i)}$ would extend to an action on E, so the resulting multiplier action by i on the tangent line $\mathrm{Lie}(E_{\mathbb{Q}(i)}) = \mathrm{Lie}(E) \otimes_R \mathbb{Q}(i)$ would preserve the R-submodule $\mathrm{Lie}(E)$. But $\mathrm{Lie}(E)$ is a free R-module of rank 1 since R is local and E is R-smooth, so the i-action on this R-module is multiplication by some element $r \in R$. By working over $\mathbb{Q}(i)$ we have seen that we get the multiplier i, so necessarily $r = i$. Since $i \notin R$ due to the definition of R, we have a contradiction.

In Example 1.8.3, the base ring R is not normal. This is essential, since in the normal case there is no obstruction to extending maps between abelian schemes:

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

PROOF. This is a special case of a general lemma of Faltings [**36**, §2, Lemma 1] concerning homomorphisms between semi-abelian schemes over a normal scheme (the proof of which simplifies considerably in the case of abelian schemes). □

1.8.4.1. For normal R, Lemma 1.8.4 provides a specialization map

$$\mathrm{End}^0(A_K) = \mathrm{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(A) \to \mathrm{End}^0(A_\kappa)$$

between endomorphism algebras, and likewise for endomorphism rings. This makes normality a natural property to impose on R when studying questions about CM lifts. If R is not normal then $\mathrm{End}^0(A_K)$ may be larger than $\mathrm{End}^0(A)$, so it is not evident how to compare endomorphism algebras of the K-fiber and κ-fiber.

Hence, for general R we just work with the specialization map of endomorphism algebras $\mathrm{End}^0(A) \to \mathrm{End}^0(A_\kappa)$. This map can fail to be surjective. An elementary example is an elliptic curve over $\mathbb{Z}_{(p)}$ for a prime p (since elliptic curves over finite fields always admit complex multiplication, by Corollary 1.6.2.5, whereas elliptic curves over $\mathbb{Q}$ have endomorphism algebra $\mathbb{Q}$). In contrast with Lemma 1.8.2, the specialization map of endomorphism rings $\mathrm{End}(A) \to \mathrm{End}(A_\kappa)$ can have cokernel that is not torsion-free, even when R is normal. (In Chapter 4 we will see many natural examples of this phenomenon in our study of CM lifting problems, when we consider lifting questions for specific orders in CM fields; e.g., see 4.1.2.)

1.8.4.2. Remark. In the setting of Lemma 1.8.4, if $\lambda : A \to B$ is a homomorphism between abelian schemes over R and λ_K is an isogeny then λ is an isogeny (i.e., λ is fiberwise surjective with finite kernel; see §3.3 for a general discussion of isogenies for abelian schemes). To prove this, choose a K-homomorphism $\mu_K : B_K \to A_K$ such that $\mu_K \circ \lambda_K$ is multiplication by a non-zero integer n. The homomorphism $\mu : B \to A$ extending μ_K therefore satisfies $\mu \circ \lambda = [n]_A$, so λ has a fiberwise finite kernel and hence is an isogeny by fibral dimension considerations.

1.8.5. CM lifting problems. To formulate the lifting questions that we study in subsequent chapters, 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 B is isotypic over $\mathbb{F}_q$ (necessary and sufficient for B to admit a structure of CM abelian variety with complex multiplication by a CM field, by Theorem 1.3.1.1 and Corollary 1.6.2.5). Let B_κ denote the scalar extension of B over a finite extension field $\kappa/\mathbb{F}_q$. Consider the following five assertions concerning the existence of a CM lifting of B or B_κ to characteristic 0.

- (CML) CM *lifting*: there is a local domain R with characteristic 0 and residue field $\mathbb{F}_q$, an abelian scheme A over R with relative dimension g equipped with a CM field $L \subset \mathrm{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(A)$ satisfying $[L : \mathbb{Q}] = 2g$, and an isomorphism $\phi : A_{\mathbb{F}_q} \simeq B$ as abelian varieties over $\mathbb{F}_q$.

- (R) CM *lifting after finite residue field extension*: there is 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 $\phi : A_\kappa \simeq B \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\kappa)$ as abelian varieties over κ.
- (I) CM *lifting up to isogeny*: there is 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 $A_{\mathbb{F}_q} \to B$ of abelian varieties over $\mathbb{F}_q$.
- (IN) CM *lifting to normal domains up to isogeny*: there is a normal local domain R with characteristic 0 and residue field $\mathbb{F}_q$ such that (I) is satisfied for B using R.
- (RIN) CM *lifting to normal domains up to isogeny after finite residue field extension*: there is 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 rather than an isomorphism.
- (sCML) *strong* CM *lifting*: For every CM field $L \subset \mathrm{End}^0(B)$ with $[L : \mathbb{Q}] = 2g$ such that $\mathcal{O}_L \subset \mathrm{End}(B)$, the abelian variety B satisfies (CML) using a lifting A such that the $\mathbb{Q}$-subalgebra $\mathrm{End}^0(A) \subset \mathrm{End}^0(B)$ contains L.

1.8.5.1. Remark. By expressing a local ring as a direct limit of local subrings essentially of finite type over $\mathbb{Z}$, in the formulation of (R) there is no loss of generality in replacing κ with an algebraic closure of $\mathbb{F}_q$ or allowing κ to vary over all extensions of $\mathbb{F}_q$. Likewise, the normality condition in (RIN) is irrelevant because it can be attained at the cost of a finite residue field extension (by a specialization argument that we will give in 2.1.1), and in (IN) we can assume R is complete since essentially finite type $\mathbb{Z}$-algebras are excellent (ensuring that normality is preserved under completion of such rings along an ideal). Even in (I) we can assume R is complete local noetherian since we may first descend to a local noetherian domain $R_0 \subset R$ of characteristic 0 with residue field $\mathbb{F}_q$, and then note that the completion $\widehat{R}_0$ of R_0 has a minimal prime of residue characteristic 0 (as $R_0 \to \widehat{R}_0$ is faithfully flat).

By Remark 1.6.5.2, (RIN) has an affirmative answer for any isotypic B over $\mathbb{F}_q$, and the CM lift can be chosen using *any* CM maximal commutative subfield $L \subset \mathrm{End}^0(B)$. There are several refinements we wish to answer:

(1) Is a residue field extension necessary? That is, does (IN) hold for every B?
(2) If (IN) does not hold for every B, can we characterize when it holds? And how about (I) in general (i.e., drop normality, but permit an isogeny without increasing the residue field)?
(3) Is an isogeny necessary? That is, does (R) hold for every B (requiring the local domain R to be normal is not a constraint, since we are allowing a finite extension on κ; cf. Remark 1.8.5.1), or does even (CML) hold for every B?

These questions can be made more specific in several respects. For example, since the $\mathbb{Q}$-simple $\mathrm{End}^0(B)$ is usually non-commutative, it generally contains more than one CM maximal commutative subfield L (up to conjugacy) and so we can pose the CM lifting questions requiring an order in a particular choice of L to lift to a CM structure over R. We will give examples to show that the choice of L can affect the the answer to some of the lifting questions. Even if we know for a given B and $L \subset \mathrm{End}^0(B)$ that there is a CM lift to characteristic 0 on which the action of an order in L also lifts, it could be that the CM order $L \cap \mathrm{End}(B)$ does not lift. We will give examples where this happens in 4.1.2 (see Theorem 4.1.1 and the non-algebraizable universal formal deformation in 4.1.2.3).

1.8.6. Answers to CM lifting problems. The proofs of the following answers form the backbone of subsequent chapters.

1. By [**93**, Thm. B], for any $g > 2$ there exist g-dimensional abelian varieties over an algebraic closure of $\mathbb{F}_p$ for which there is no CM lift to characteristic 0. These results are proved in a much stronger form in Chapter 3. Thus, (R) does not hold in general, so in particular (CML) sometimes fails to hold. Hence, *an isogeny is necessary*; that is, it is better to consider (I) than (CML).
2. Building on lifting results for p-divisible groups in Chapter 3, in Chapter 4 we prove that (I) holds for every B (so a strengthening of (RIN) holds, applying the isogeny before making a finite extension on the residue field). In fact, for any CM maximal commutative subfield $L \subset \mathrm{End}^0(B)$ we construct an isogeny $B \to B'$ to an abelian variety over $\mathbb{F}_q$ such that B' has a CM lift to characteristic 0 on which the action of the order $\mathbb{Z} + p\mathcal{O}_L$ in $\mathcal{O}_L$ also lifts.

   The abelian variety B' generally depends on L, but we can arrange that the isogeny to B' is a p-power at most p^{4g^2} (and examples show that we cannot arrange it to have degree not divisible by p in general). The CM lifting of B' can be found over an order in a p-adic field whose relative ramification degree over a specific p-adic reflex field is tightly controlled (usually 1).
3. In contrast with success for (I), if we require R to be normal and do not increase the residue field (but permit isogenies) then the answer is negative: in Chapter 2 we give examples for which (IN) fails. Hence, for the existence of a CM lifting to a normal domain of characteristic 0 we must allow a finite extension of the initial finite field (and an isogeny), as in Theorem 1.6.5.1.

   However, there is a salvage: for each B and choice of $L \subset \mathrm{End}^0(B)$ we will give (in Chapter 2) concrete *necessary and sufficient* conditions in terms of a $\overline{\mathbb{Q}}_p$-valued CM type Φ on L for (IN) to have an affirmative answer using a CM lifting to which the action of an order in L (in the isogeny category) also lifts and yields the specified CM type Φ. In Example 2.1.7 we will give B for which this necessary and sufficient condition is satisfied for one choice of $L \subset \mathrm{End}^0(B)$ (and a suitable Φ) but fails for another choice (and any Φ).

We expect that (sCML) in 1.8.5 does *not* hold in general, but this is a guess.

1.8.7. Remark. (CM types in (IN) and (I)). In the context of 1.8.5, for any CM structure $L \subset \mathrm{End}^0(B)$ on the abelian variety B the q-Frobenius endomorphism $\varphi \in \mathrm{End}(B)$ lies in $L^\times$ since L is its own centralizer in $\mathrm{End}^0(B)$. The combinatorial data of L-*slopes* of the L-linear isogeny class of $(B, L \subset \mathrm{End}^0(B))$ is the sequence of non-negative rational numbers $r_w = \mathrm{ord}_w(\varphi)/\mathrm{ord}_w(q)$ indexed by the set of places w of L above p. When L is a CM field, with complex conjugation ι, this satisfies the self-duality condition $r_w + r_{w\circ\iota} = 1$ for each w (since $\varphi \cdot \iota(\varphi) = q$ in L).

Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and an embedding of $\mathbb{F}_q$ into the residue field of the valuation ring of $\overline{\mathbb{Q}}_p$ (so $W(\mathbb{F}_q)[1/p]$ canonically embeds into $\overline{\mathbb{Q}}_p$). For any

CM lifting of $(B, L \subset \mathrm{End}^0(B))$ over the valuation ring of a subfield of $\overline{\mathbb{Q}}_p$ of finite degree over $W(\mathbb{F}_q)[1/p]$, the associated $\overline{\mathbb{Q}}_p$-valued CM type Φ on L must satisfy the following compatibility condition with the L-slopes:

$$\#\{\phi \in \Phi \mid \phi \text{ induces } w \text{ on } L\} = r_w$$

for all w; see 2.1.4.1–2.1.4.2. For any $\overline{\mathbb{Q}}_p$-valued CM type (L, Φ) satisfying this necessary condition, in Chapter 2 we prove a necessary and sufficient condition for the existence of a solution $\mathcal{B}$ to problem (IN) for (B, L) over a local normal domain $R \supseteq W(\mathbb{F}_q)$ with residue field $\mathbb{F}_q$ such that the L-action (in the isogeny category) lifts to $\mathcal{B}$ and the resulting CM structure over $K = \mathrm{Frac}(R)$ has $\overline{\mathbb{Q}}_p$-valued CM type Φ relative to some $W(\mathbb{F}_q)[1/p]$-algebra embedding of $\overline{\mathbb{Q}}_p$ into $\overline{K}$.

Without normality it is more difficult to determine which CM types on L arise from solutions to the lifting problem (I) for (B, L) when we require the L-action to lift. If L is a CM field, the answer is p-local for the maximal totally real subfield L^+: it can be analyzed separately for each p-adic place v of L^+. To be precise, a $\overline{\mathbb{Q}}_p$-valued CM type Φ for L corresponds to a sequence $\{(L_v^+ \otimes_{L^+} L, \Phi_v)\}_v$ where Φ_v is a set of $\mathbb{Q}_p$-algebra homomorphisms $L_v^+ \otimes_{L^+} L \to \overline{\mathbb{Q}}_p$, and via p-divisible groups the question reduces to determining (for each v) the family $\mathfrak{F}_v$ of all Φ_v that arise as the v-component of the $\overline{\mathbb{Q}}_p$-valued CM type of an affirmative solution to the CM lifting problem (I) for the CM structure $(B, L \subset \mathrm{End}^0(B))$.

When v is split in L, say with w and w' the two places over it on L, there turn out to be no restrictions on Φ_v beyond the above compatibility conditions

$$r_w = \#\{\phi \in \Phi_v \mid \phi \text{ induces } w \text{ on } L\}, \;\; r_{w'} = \#\{\phi \in \Phi_v \mid \phi \text{ induces } w' \text{ on } L\}$$

(which can always be satisfied, since any $\phi \in \Phi_v$ induces w or w' on L). However when v is non-split in L, the proofs in Chapter 4, B.1, and B.2 provide only a non-empty subset $\mathfrak{F}'_v$ of $\mathfrak{F}_v$;[3] we do not know the discrepancy between $\mathfrak{F}_v$ and $\mathfrak{F}'_v$.[4]

[3]The set $\mathfrak{F}'_v$ is the family of all v-components of $\mathbb{Q}_p$-valued CM types of affirmative solutions to (I) which can be constructed by the method in B.1 and B.2 together with the Serre tensor construction for p-divisible groups in 4.3. The proof in Chapter 4, especially 4.5.15 (iii)–4.5.17, which uses the Serre tensor construction and the existence of CM lifting of toy model p-divisible groups, gives a non-empty subset $\mathfrak{F}''_v$ of $\mathfrak{F}'_v$ which can be strictly smaller than $\mathfrak{F}'_v$.

[4]A complete solution of (sCML) should also provide an answer to this question.