Bulletin of the Institute of Mathematics
Academia Sinica (New Series)
Vol. **15** (2020), No. 1, pp. 9-32
DOI: 10.21915/BIMAS.2020102

A NOTE ON SUPERSINGULAR ABELIAN VARIETIES

CHIA-FU YU

Institute of Mathematics, Academia Sinica and NCTS, Taipei, Taiwan
E-mail: chiafu@math.sinica.edu.tw

Abstract

In this note we show that every supersingular abelian variety is isogenous to a superspecial abelian variety without increasing field extensions. The proof uses minimal isogenies and Galois descent. We construct a superspecial abelian variety which cannot be descended to a finite field. This answers negatively to a question of the author in [J. Pure Appl. Alg., 2013]. Endomorphism algebras of supersingular elliptic curves over an arbitrary field are investigated. We correct the main result of the author's paper [Math. Res. Let., 2010].

1. Introduction

Throughout this note, p denotes a prime number and all ground fields considered are of characteristic p, unless specifically stated otherwise. We discuss endomorphism algebras and fields of definition of supersingular isogeny classes. There are several equivalent definitions for supersingular abelian varieties. We use the definition that an abelian variety A over a field $k \supset \mathbb{F}_p$ is said to be *supersingular* if its associated p-divisible group $A[p^\infty]$ has only one slope $1/2$. This definition is well defined in the sense that it does not depend on the ground field over which A is defined. However, the definition requires the prerequisites of Dieudonné module theory and the Manin-Dieudonné classification of p-divisible groups up to isogeny. Oort [12] showed that every supersingular abelian variety over an algebraically closed field is isogenous to a product of supersingular elliptic curves. This provides an alternative but much simpler definition. Our discussion starts with the following result of Deligne, Ogus and Shioda (cf. [7, Section 1.6, p. 13]).

Received October 15, 2019.
AMS Subject Classification: 14K15, 11G10.
Key words and phrases: Supersingular abelian varieties, Galois descent.

Theorem 1.1. *For every integer $g \geq 2$ and any supersingular elliptic curves E_i over an algebraically closed field k for $1 \leq i \leq 2g$, one has $E_1 \times \cdots \times E_g \simeq E_{g+1} \times \cdots \times E_{2g}$.*

Let E_0 be a supersingular elliptic curve over $\mathbb{F}_p$ such that its Frobenius endomorphism π_{E_0} satisfies $\pi_{E_0}^2 + p = 0$. Then every supersingular abelian variety A over an algebraically closed field k can be obtained by an isogeny

$$\varphi : E_0^g \otimes_{\mathbb{F}_p} k \to A, \tag{1.1}$$

where $g = \dim A$. Equivalently, if A is a supersingular abelian variety over a field k, not necessarily algebraically closed, then there exists a finite field extension k_1/k and a k_1-isogeny

$$\varphi : E_0^g \otimes_{\mathbb{F}_p} k_1 \to A \otimes_k k_1. \tag{1.2}$$

We show the alterations from $E_0^g \otimes k$ by a finite field extension base change and by an isogeny are all necessary. For example, if A is k-simple, then A cannot be isogenous to $E_0^g \otimes_{\mathbb{F}_p} k$. One can easily construct an $\mathbb{F}_q$-simple supersingular abelian variety using the Honda-Tate theorem [17]. On the other hand, the "moduli space" of supersingular abelian varieties of dimension $g > 1$ has positive dimension, while the locus which consists of superspecial abelian varieties is zero-dimensional. This shows that a modification by an isogeny is also necessary. An abelian variety A over k is said to be *superspecial* if $A \otimes_k \bar{k}$ is isomorphic to a product of supersingular elliptic curves, where $\bar{k}$ denotes an algebraic closure of k.

We say that an algebraic variety (or a scheme) X over a field k *can be descended* to a subfield k_0 of k if there is an algebraic variety (or a scheme) X_0 over k_0 and a k-isomorphism $X_0 \otimes_{k_0} k \simeq X$. In this case, X_0 is called a *model* of X over k_0 and we say X is *defined over* k_0. If the base change $X \otimes_k \bar{k}$ has a model over k_0, we say X is *defined over* k_0 *after a base change*, in order to distinguish the previous notion. In some literature, the terminology "X is defined over k_0" actually means that X is defined over k_0 after a base change in our definition. *The field of moduli of* X, denoted by $\mathrm{fom}(X)$, is the smallest subfield k_0 of $\bar{k}$ such that $(X \otimes_k \bar{k})^\sigma \simeq X \otimes_k \bar{k}$ for all $\sigma \in \mathrm{Aut}(\bar{k}/k_0)$.

We have

$$\begin{aligned} X \text{ is defined over } k_0 &\implies X \text{ is defined over } k_0 \text{ after a base change} \\ &\implies \operatorname{fom}(X) \subset k_0. \end{aligned}$$

These three concepts are different. For example, every elliptic curve E over a field $k \supset \mathbb{F}_p$ is defined over $\mathbb{F}_p(j_E)$ after a base change and the subfield $\mathbb{F}_p(j_E)$ is also the field of moduli of E, where j_E is the j-invariant of E. However, E cannot be descended to $\mathbb{F}_p(j_E)$ from k in general.

We are interested in computing the endomorphism algebra of a supersingular abelian variety over an arbitrary field k. For this purpose, the description (1.2) does not help at all. We would like to know

Question (A): Is every supersingular abelian variety A over k k-isogenous to an abelian variety A' which can be defined over a finite subfield of k?

Question (B): Is every supersingular abelian variety over k is k-isogenous to a superspecial abelian variety over k?

If Question (A) has an affirmative answer, then the endomorphism algebra of A is isomorphic to the endomorphism algebra of another supersingular abelian variety A' over a finite field. By a theorem of Manin and Oort, any supersingular Weil q-number π, that is, its conjugacy class corresponds to a simple supersingular isogeny class, is of the form $\sqrt{q}\zeta$, where ζ is a root of unity; see [12, p. 116] (also [25, Theorem 2.8]). Using Tate's theorem on endomorphism algebras [16, p. 142], one can determine its endomorphism algebra. Except the case where $\pi = \sqrt{q} \notin \mathbb{Q}$, the endomorphism algebra of any simple supersingular abelian variety over $\mathbb{F}_q$ either an abelian CM field or a quaternion division algebra over a cyclotomic field [21, Sect. 3]. Using the Poincare irreducibility theorem. the endomorphism algebra of A is isomorphic to a finite product of $\mathbb{Q}$-simple algebras of the form $\operatorname{Mat}_n(D)$, where D is one of the following four cases:

(1) the definite quaternion $\mathbb{Q}$-algebra $B_{p,\infty}$ ramified exactly at $\{p, \infty\}$;
(2) the definite quaternion $\mathbb{Q}(\sqrt{p})$-algebra D_{∞_1,∞_2} ramified only at the two real places $\{\infty_1, \infty_2\}$ of $\mathbb{Q}(\sqrt{p})$;
(3) an abelian CM field; or

(4) a quaternion division algebra over a cyclotomic field ramified only at places over p.

Concerning our questions, we prove the following result.

Theorem 1.2.

(1) *Let A be a supersingular abelian variety over a field k. There exists a superspecial abelian variety C over k and a k-isogeny $A \to C$.*

(2) *There exists a supersingular abelian variety A over some field k such that for any k-isogeny $A \sim A'$ of abelian varieties, A' is not defined over a finite field.*

We write $\mathrm{End}(A)$ for the endomorphism ring of A over k and $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ for its endomorphism algebra. For any field extension k' of k, we write $\mathrm{End}(A \otimes_k k')$, instead of $\mathrm{End}_{k'}(A)$, for the endomorphism ring of $A \otimes_k k'$ over k'.

By Theorem 1.2 (1), any supersingular abelian variety over k can be parametrized by a pair (A_0, φ), where A_0 is a superspecial abelian variety over k and $\varphi : A_0 \to A$ is a k-isogeny. If $g > 1$, then any such A_0 is a k-form of $E_0^g \otimes k$ and these k-forms are classified by the Galois cohomology $H^1(k, \mathrm{GL}_g(\mathcal{O}))$, where $\mathcal{O} := \mathrm{End}(E_0 \otimes k_s)$ and k_s is a separable closure of k. The endomorphism algebra $\mathrm{End}^0(E_0 \otimes k_s)$ is isomorphic to $B_{p,\infty}$ and $\mathcal{O}$ is a maximal order. In the case that $k \supset \mathbb{F}_{p^2}$, the Galois group $\Gamma_k := \mathrm{Gal}(k_s/k)$ acts trivially on $\mathrm{GL}_g(\mathcal{O})$ and we have

$$H^1(k, \mathrm{GL}_g(\mathcal{O})) = \mathrm{Hom}(\Gamma_k, \mathrm{GL}_g(\mathcal{O}))/\mathrm{GL}_g(\mathcal{O}),$$

which parameterizes conjugacy classes of finite subgroups H in $\mathrm{GL}_g(\mathcal{O})$ which occur as quotients of Γ_k. From this approach, the inverse Galois problem comes into play.

We will see that there exists a superspecial abelian variety which is not defined a finite field (Remark 4.4 (2)). We construct such an example in Section 4. This answers negatively to a question in [25, (Q), p. 912]. The construction uses arithmetic properties of definite quaternion $\mathbb{Q}$-algebras and an explicit computation of Galois cohomology.

An abelian variety A is said to *have smCM* if the endomorphism algebra $\mathrm{End}^0(A)$ of A contains a commutative semi-simple $\mathbb{Q}$-subalgebra L of degree

$2 \dim A$. In this case L can be chosen to be a CM algebra. A theorem of Grothendieck states that if A is an abelian variety with smCM over a field k, then there is a finite field extension k_1/k, an abelian variety A_0 over a finite field $k_0 \subset k_1$ and a k_1-isogeny $\varphi : A \otimes_k k_1 \to A_0 \otimes_{k_0} k_1$; see [10, pp. 220/221], [11, Theorem 1.1] and [22, Theorem 1.4]. Similar to supersingular abelian varieties, the conditions "up to isogeny" and "up to a finite extension" in Grothendieck's theorem for smCM abelian varieties are all necessary. For example, a geometric generic supersingular abelian surface is not defined over a finite field and hence the first condition is necessary. We show in Section 4 by giving an example that the second condition "up to a finite extension" is also necessary.

As a consequence of Theorem 1.2 (1), one can in principle compute the endomorphism algebra of any supersingular abelian variety. Inspired from Theorem 1.2 (2), we would like to know

Question (C): Is there a supersingular abelian variety A over a field k such that its endomorphism algebra $\mathrm{End}^0(A)$ is not isomorphic to the endomorphism algebra of a supersingular abelian variety of the same dimension over a finite field?

We also would like to know

Question (D): Let A be a smCM abelian variety over a field k. Is its endomorphism algebra $\mathrm{End}^0(A)$ isomorphic to the endomorphism algebra of an abelian variety of the same dimension over a finite field?

We examine the case where $g = 1$ and obtain the following result. We wish to explore some higher-dimensional cases along this direction.

Theorem 1.3.

(1) *If* $p \not\equiv 1 \pmod{12}$*, then there is a supersingular elliptic curve* E *over a field* k *such that* $\mathrm{End}^0(E) = \mathbb{Q}$*.*

(2) *If* $p \equiv 1 \pmod{12}$*, then for any supersingular elliptic curve* E *over an arbitrary field* k*, one has* $\mathrm{End}^0(E) \neq \mathbb{Q}$*. Moreover,* $\mathrm{End}^0(E)$ *is either isomorphic to the definite quaternion* $\mathbb{Q}$*-algebra* $B_{p,\infty}$ *ramified exactly at* $\{p, \infty\}$*, or a two-dimensional subfield of* $B_{p,\infty}$*.*

Theorem 1.3 shows that Question (C) has an affirmative answer in the case where $p \not\equiv 1 \pmod{12}$. Our proof of Theorem 1.3 (2) also gives all possible $\mathbb{Q}$-algebras that can occur as the endomorphism algebra of a supersingular elliptic curve over an arbitrary field when $p \equiv 1 \pmod{12}$. Furthermore, all of them also occur as the endomorphism algebras of those which are defined over finite fields. Thus, Question (D) has an affirmative answer in this case.

Due to the positive answer to Question (C), we would like to know

Question (E): For each integer d and each prime p, what are the endomorphism algebras of d-dimensional supersingular abelian varieties over a field k of characteristic p?

We have described the list of them when k is a finite field above. The following result gives a new example.

Theorem 1.4 (cf. Theorem 6.1)**.** *For every positive integer d and every prime $p \not\equiv 1 \pmod{12}$ there exists a supersingular abelian variety A of dimension d over a field k of characteristic p such that* $\mathrm{End}^0(A) = \mathbb{Q}$.

2. Minimal Isogenies over Perfect Fields

In this section, we show the existence of minimal isogenies for abelian varieties and p-divisible groups over perfect fields. This generalizes previous results of the author [23] where the ground field is assumed to be algebraically closed. A special case of this result will be used in the proof of Theorem 1.2 (1).

Let k be a perfect field of characteristic p. Let $W := W(k)$ be the ring of Witt vectors over k, and $B(k)$ the fraction field of $W(k)$. Let σ be the Frobenius map on W and $B(k)$, respectively. We use the covariant Dieudonné theory [27]. Dieudonné modules considered here are assumed to be finite and free as W-modules.

To each rational number $0 \leq \lambda \leq 1$, one associates a pair (a, b) of coprime non-negative integers so that $\lambda = b/(a+b)$. For each pair $(a, b) \neq (0, 0)$ as above, write $M_{(a,b)}$ for the Dieudonné module $W[F, V]/(F^a - V^b)$ over k of slope $\lambda = b/(a+b)$.

We write a Newton polygon of slopes in $[0,1]$ as a finite formal sum $\beta = \sum_{i=1}^{s} r_i(a_i, b_i)$, or express it in terms of a slope sequence $\beta = (\lambda_1^{(r_1(a_1+b_1))}, \ldots, \lambda_s^{(r_s(a_s+b_s))})$, where each $0 \leq \lambda_i \leq 1$ is a rational number with $\lambda_i < \lambda_{i+1}$, $r_i \in \mathbb{N}$ is a positive integer, and (a_i, b_i) is the pair associated to λ_i (By convention, the multiplicity of the slope λ_i is $(a_i + b_i)r_i$). Let M be a Dieudonné module over k and put $N := M \otimes_W B(k)$. By the Manin-Dieudonné Theorem ([9], Chap. II, "Classification Theorem", p. 35), the isocrystal $N' := N \otimes_{B(k)} B(k')$, where $k' \supset k$ is an algebraically closed overfield, admits a unique decomposition

$$N' = \oplus_i N'_{\lambda_i}, \quad N'_{\lambda_i} \simeq (M_{(a_i,b_i)} \otimes_W B(k'))^{r_i}, \tag{2.1}$$

for some Newton polygon $\beta = \sum_i r_i(a_i, b_i)$. The invariant β is independent of the choice of k' and is called the *Newton polygon* of M. By the existence of slope filtration for Dieudonné modules and the splitting theorem up to isogeny [6, Theorem 2.5.1], the decomposition (2.1) is actually defined over $B(k)$. Namely, one has a unique decomposition of N into isotypic components

$$N = \oplus_i N_{\lambda_i}, \quad N_{\lambda_i} \otimes_{B(k)} B(k') = N'_{\lambda_i}. \tag{2.2}$$

See Zink [26] and Oort and Zink [14] for a far generalization of the slope filtration for p-divisible groups over normal base schemes.

Let $(a, b) \neq (0, 0) \in (\mathbb{Z}_{\geq 0})^2$ be a pair as before, and put $n = a + b$. Denote by $\mathbf{M}_{(a,b)}$ the Dieudonné module over $\mathbb{F}_p$ generated by the elements e_i, for $i \in \mathbb{Z}_{\geq 0}$, with relation $e_{i+n} = pe_i$, as a $\mathbb{Z}_p$-module, and with operations $Fe_i = e_{i+b}$ and $Ve_i = e_{i+a}$ for all $i \in \mathbb{Z}_{\geq 0}$. Clearly, $F^n = p^b$ and $V^n = p^a$ on $\mathbf{M}_{(a,b)}$. For each Newton polygon $\beta = \sum_{i=1}^{s} r_i(a_i, b_i)$, define

$$\mathbf{M}(\beta) := \bigoplus_{i=1}^{s} \mathbf{M}_{(a_i,b_i)}^{r_i}.$$

Let M_λ be an isoclinic Dieudonné module over k of slope slope $\lambda = b/(a + b)$. There are two integers x and y such that $bx + ay = 1$. We define a σ^{x-y}-linear operator on $N_\lambda := M_\lambda \otimes_W B(k)$ by

$$\Phi_\lambda = F^x V^y : N_\lambda \to N_\lambda. \tag{2.3}$$

If $M_\lambda = \mathbf{M}_{(a,b)}$, then one has $\Phi_\lambda(e_i) = e_{i+1}$ for all i.

Definition 2.1. A Dieudonné module M over k with Newton polygon β is said to be *minimal* if for any algebraically closed field $k' \supset k$, one has $M \otimes_W W(k') \simeq \mathbf{M}(\beta) \otimes_{\mathbb{Z}_p} W(k')$.

Lemma 2.2. *Let M be a Dieudonné module over an algebraically closed field k with Newton polygon β. The following are equivalent:*

(a) *There is an isomorphism $M \simeq \mathbf{M}(\beta) \otimes_{\mathbb{Z}_p} W(k)$ of Dieudonné modules.*

(b) *The endomorphism ring $\mathrm{End}(M)$ is a maximal order of the endomorphism algebra $\mathrm{End}^0(M) = \mathrm{End}(M) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of M.*

(c) *M is the direct sum of its isotypic components M_λ and each component M_λ is a minimal Dieudonné module.*

If M is isoclinic with slope $\lambda = b/(a+b)$, then the statement (a), (b), *or* (c) *is equivalent to*

(d) *$F^{a+b}M = p^b M$ and $\Phi_\lambda(M) \subset M$, where Φ_λ is defined in* (2.3).

Proof. See [23, Lemmas 3.3 and 3.4]. □

By Lemma 2.2, a Dieudonné module M over k is minimal if and only if so is $M \otimes_W W(k') \simeq \mathbf{M}(\beta) \otimes_{\mathbb{Z}_p} W(k')$ for one algebraically closed field $k' \supset k$.

Definition 2.3 (cf. [7, Section 1] and [23, Section 4])**.** Let X be a p-divisible group over a field k_1 of characteristic p.

(1) We say that X is *minimal* if the Dieudonné module of $X \otimes_{k_1} \bar{k}_1$ satisfies one of the equivalent conditions in Lemma 2.2.

(2) The *minimal isogeny* of X is a pair (X_0, φ), where X_0 is a minimal p-divisible group over k_1, and $\varphi : X_0 \to X$ is an isogeny over k_1 such that for any other pair (X_0', φ') as above, there exists an isogeny $\rho : X_0' \to X_0$ such that $\varphi' = \varphi \circ \rho$. Note that the morphism ρ is unique if it exists.

Lemma 2.4. *Let M be a Dieudonné module over a perfect field k with Newton polygon β. Then there exists a unique smallest minimal Dieudonné module $M^{\min}$ over k containing M. Dually, there is a unique largest minimal Dieudonné submodule $M_{\min}$ of M.*

Proof. We first show that if M_1 and M_2 are minimal Dieudonné modules (of full rank) in $N := M \otimes B(k)$ then so are $M_1 + M_2$ and $M_1 \cap M_2$. For any algebraically closed overfield k', put $M_i' := M_i \otimes W(k')$ for $i = 1, 2$. Clearly we have $(M_1+M_2)\otimes W(k') = M_1'+M_2'$ and $(M_1\cap M_2)\otimes W(k') = M_1'\cap M_2'$ in N. Thus, we are reduced to the case where k is algebraically closed and this follows from Lemma 2.2 as both $M_1 + M_2$ and $M_1 \cap M_2$ satisfy the criterion (d). Therefore, the uniqueness of $M^{\min}$ has been proved and it remains to show that there is a minimal Dieudonné module over k containing M.

Put $M_\lambda = M \cap N_\lambda$ and by (2.2) we have $M \subset \oplus_\lambda M_\lambda$, where N_λ is the isotypic component of N of slope λ. It then suffices to show that each M_λ is contained in a minimal Dieudonné module, and we can assume that $M = M_\lambda$ is isoclinic of slope $\lambda = b/(a + b)$. Let $P(M)$ be the W-submodule generated by M which is stable under the operators $F^{a+b}p^{-b}$ and Φ_λ. By [23, Lemma 4.2], the Dieudonné module $M \otimes_W W(k')$ is contained in a minimal Dieudonné module, which is stable under these operators. Thus, $P(M) \otimes W(k') \subset M_0'$. It follows that $P(M)$ is a W-module of finite rank and it is a Dieudonné module. As $P(M) \otimes W(k')$ is a Dieudonné module stable under $F^{a+b}p^{-b}$ and Φ_λ, it follows from Lemma 2.2 that $P(M)$ is minimal. □

The minimal Dieudonné module $M_{\min}$ (resp. $M^{\min}$) constructed in Lemma 2.4 is called the *minimal Dieudonné submodule* (resp. *overmodule*) of M. By Lemma 2.4, we have

Corollary 2.5. *The minimal isogeny of any p-divisible group X over k exists.*

Let $\mathcal{O}$ be an order of a finite-dimensional semi-simple algebra over $\mathbb{Q}_p$. A p-divisible $\mathcal{O}$-module is a pair (X, ι), where X is a p-divisible group and $\iota : \mathcal{O} \to \mathrm{End}(X)$ is a ring monomorphism.

Proposition 2.6. *Let (X, ι) be a p-divisible $\mathcal{O}$-module over k and let $\varphi : X_0 \to X$ be the minimal isogeny of X over k. Then there is a unique ring monomorphism $\iota_0 : \mathcal{O} \to \mathrm{End}(X_0)$ such that φ is $\mathcal{O}$-linear.*

Proof. The same statement is proved in [23, Prop. 4.8] where the ground field is assumed to be algebraically closed. The same proof also works for the present situation. □

Remark 2.7. In [4], S. Harashita shows that any p-divisible group over an arbitrary field k of characteristic p is k-isogenous to a minimal p-divisible group. His result may be used to improve Corollary 2.5 and Proposition 2.6 without the perfectness assumption of the ground field. Note that for the purpose of computing endomorphism algebras of abelian varieties as we are, one can always assume that the ground field is perfect by Lemma 3.2.

3. Proof of Theorem 1.2 (2)

Lemma 3.1. *Let A be a supersingular abelian variety of dimension g over a field k of characteristic p. There is a finite purely inseparable extension field L/k and an L-isogeny $A_L = A \otimes_k L \to B$, where B is a superspecial abelian variety over L.*

Proof. Let k' be the perfect closure of k. It suffices to show that there is a k'-isogeny $\varphi : A_{k'} \to B$ for a superspecial abelian variety B over k' because $\ker\varphi$ is defined over a finite extension L of k in k' and hence both B and φ are defined over L, which is purely inseparable over k. Let M be the covariant Dieudonné module of $A_{k'}$. By Lemma 2.4, M is contained in a superspecial Dieudonné module M' over k'. Therefore there is an (necessarily superspecial) abelian variety B over k' and a k-isogeny $\varphi : A_{k'} \to B$ which realizes the chain of Dieudonné modules $M \subset M'$. □

Lemma 3.2. *Let A_1 and A_2 be two abelian varieties over k and L/k a primary field extension (i.e. k is separably algebraically closed in L). Then we have an isomorphism*

$$\mathrm{Hom}_k(A_1, A_2) \xrightarrow{\sim} \mathrm{Hom}_L(A_{1,L}, A_{2,L}).$$

Proof. See [2, Lemma 1.2.1.2]. A key ingredient is that the Hom-scheme $\underline{\mathrm{Hom}}_k(A_1, A_2) \to \mathrm{Spec}\, k$ is unramified. This follows from the rigidity of endomorphisms of abelian schemes. □

Lemma 3.3. *Let L/k be a finite purely inseparable extension field and B a superspecial abelian variety over L of dimension $g \geq 2$. Then there exists an abelian variety B' over k and an L-isomorphism $B'_L \simeq B$.*

Proof. Take any superspecial abelian variety A over k of dimension g. For example let $A = E^g \otimes_{\mathbb{F}_p} k$, where E is a supersingular elliptic curve over $\mathbb{F}_p$. By Theorem 1.1, there is a finite field extension K over L and a K-isomorphism $\varphi : B_K \simeq A_L \otimes_L K$. By Lemma 3.2, the isomorphism φ is defined over the maximal separable extension L_s of L in K. Replacing K by L_s and L_s by its Galois closure we may assume that K is finite Galois over L. We review B as a K/L-form of A_L and there is a corresponding 1-cocycle $\{\xi_\sigma\}$ of $\mathrm{Gal}(K/L)$ with values in $\mathrm{Aut}(A_K)$. Let K_1 be the maximal separable field extension of k in K; it is the field generated by sufficiently high p-th powers of elements of K over k. Then K/K_1 is a purely inseparable field extension of degree $[L : k]$, L and K_1 are linearly disjoint over k, and the restriction gives an isomorphism $\mathrm{Gal}(K/L) \simeq \mathrm{Gal}(K_1/k)$:

$$\begin{array}{ccc} L & \xrightarrow{\mathrm{Gal}} & K \\ \uparrow{\scriptstyle \mathrm{insep}} & & \uparrow{\scriptstyle \mathrm{insep}} \\ k & \xrightarrow[\mathrm{Gal}]{} & K_1\,. \end{array}$$

Identifying $\mathrm{Gal}(K/L)$ with $\mathrm{Gal}(K_1/k)$, and $\mathrm{Aut}(A_K)$ with $\mathrm{Aut}(A_{K_1})$ due to Lemma 3.2, we regard $\{\xi_\sigma\}$ as a 1-cocycle of $\mathrm{Gal}(K_1/k)$ with values in $\mathrm{Aut}(A_{K_1})$. By Galois descent there is an abelian variety B' over k corresponding to $\{\xi_\sigma\}$. As B'_L and B give rise to the same 1-cocycle, they are isomorphic. □

Proof of Theorem 1.2 (1) There is nothing to prove if $g = \dim(A) = 1$; we may assume that $g \geq 2$. By Lemma 3.1, there is a superspecial abelian variety B over a finite purely inseparable field extension L/k and an L-isogeny $A_L \to B$. By Lemma 3.3, there is a superspecial abelian variety C over k and an L-isomorphism $B \simeq C_L$. Thus, there is an L-isogeny $\varphi : A_L \to C_L$. By Lemma 3.2, φ is defined over k. □

4. Construction of Examples for Theorem 1.2 (2)

We recall briefly Galois descent. Let X_0 be a quasi-projective algebraic variety over a field k and K/k a finite Galois extension with group $\mathrm{Gal}(K/k)$. Write $X_{0K} := X_0 \otimes_k K$. Let $E(K/k, X_0)$ denote the set of k-isomorphism

classes of K/k-forms X of X_0, i.e. $X \otimes_k K$ is isomorphic to X_{0K} over K. There is a natural bijection

$$E(K/k, X_0) \xrightarrow{\sim} H^1(\mathrm{Gal}(K/k), \mathrm{Aut}(X_{0K})), \quad [X_0] \mapsto [\mathrm{id}_{X_0}]. \tag{4.1}$$

Suppose X_0' is a quasi-projective variety over k and $\eta : X_{0K} \xrightarrow{\sim} X_0' \otimes_k K$ is a K-isomorphism. For any $\sigma \in \mathrm{Gal}(K/k)$, put $a_\sigma := \eta^{-1} \circ \sigma(\eta) \in \mathrm{Aut}(X_{0K})$. Then $\{a_\sigma\}$ is a 1-cocycle with values in $\mathrm{Aut}(X_{0K})$, i.e. one has $a_{\sigma\tau} = a_\sigma \sigma(a_\tau)$, for $\sigma, \tau \in \mathrm{Gal}(K/k)$. The class of $\{a_\sigma\}$ in $H^1(\mathrm{Gal}(K/k), \mathrm{Aut}(X_{0K}))$ is uniquely determined by the k-isomorphism class of X_0'. Conversely, Galois descent asserts that any 1-cocycle $\{a_\sigma\}$ with values in $\mathrm{Aut}(X_{0K})$ is represented by a pair (X_0', η) as above. This describes the bijection (4.1).

Let $\mathrm{End}(X)$ denote the monoid of all k-morphisms from a variety X/k to itself.

Lemma 4.1. *Let $X_0' \in E(K/k, X_0)$ and $\{\xi_\sigma\}$ a 1-cocycle associated to X_0'. Then there is an isomorphism of monoids*

$$\mathrm{End}(X_0') \simeq \{a \in \mathrm{End}(X_0 \otimes K) \mid \xi_\sigma \sigma(a) \xi_\sigma^{-1} = a, \forall\, \sigma \in \mathrm{Gal}(K/k)\}. \tag{4.2}$$

Proof. Choose an isomorphism $\eta : X_{0K} \simeq X_{0K}'$ such that $\xi_\sigma = \eta^{-1}\sigma(\eta)$. We have an isomorphism $\alpha : \mathrm{End}(X_{0K}') \simeq \mathrm{End}(X_{0K})$ by $\alpha(a') := \eta^{-1} a' \eta$, i.e. there is a commutative diagram

$$\begin{array}{ccc} X_{0K} & \xrightarrow{\eta} & X_{0K}' \\ \downarrow{\scriptstyle \alpha(a')} & & \downarrow{\scriptstyle a'} \\ X_{0K} & \xrightarrow{\eta} & X_{0K}'. \end{array}$$

Put $a = \alpha(a') = \eta^{-1} a' \eta$ and $b = \alpha(\sigma(a')) = \eta^{-1}\sigma(a')\eta$. One has

$$\sigma(a) = \sigma(\eta^{-1})\sigma(a')\sigma(\eta) = \sigma(\eta^{-1})\eta[\eta^{-1}\sigma(a')\eta]\eta^{-1}\sigma(\eta) = \xi_\sigma^{-1} \cdot b \cdot \xi_\sigma.$$

That is, if one identifies $\mathrm{End}(X_{0K}')$ with $\mathrm{End}(X_{0K})$ by α, then the new $\mathrm{Gal}(K/k)$-action on $\mathrm{End}(X_{0K})$ induced from the form X_0' is given by $\sigma : a \mapsto \xi_\sigma \sigma(a) \xi_\sigma^{-1}$. Thus,

$$\begin{aligned} \mathrm{End}(X_0') &= \{a' \in \mathrm{End}(X_0' \otimes K) \mid \sigma(a') = a', \forall\, \sigma \in \mathrm{Gal}(K/k)\} \qquad (4.3) \\ &\xrightarrow{\sim} \{a \in \mathrm{End}(X_0 \otimes K) \mid \xi_\sigma \sigma(a) \xi_\sigma^{-1} = a, \forall\, \sigma \in \mathrm{Gal}(K/k)\}. \quad \square \end{aligned}$$

We now construct a supersingular abelian variety satisfying the property in Theorem 1.2 (2). More precisely, for each prime p, we first find a supersingular elliptic curve in characteristic p which cannot be descended to a finite subfield. We then produce superspecial abelian varieties with this property using a more result (see Proposition 4.3).

Choose a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$ with Frobenius endomorphism $\pi_{E_0} = -p$. Then $\mathrm{End}^0(E_0) \simeq B_{p,\infty}$ and $\mathrm{End}(E_0)$ is a maximal order. Put $G = \mathrm{Aut}(E_0)$.

Choose an integer $m > 1$ with $m \mid p^2 - 1$ and an element $\zeta \in \mathbb{F}_{p^2}^{\times}$ of order m. Such an integer m always exists for any prime p; for example let $m = 3$ if $p = 2$, and $m = 2$ if p is odd. Consider $k := \mathbb{F}_{p^2}(T)$ and $K := \mathbb{F}_{p^2}(T^{1/m})$, where T is a variable. Then K/k is a cyclic extension with Galois group $\mathrm{Gal}(K/k) = \langle \sigma_m \rangle$, where $\sigma_m(T^{1/m}) = \zeta T^{1/m}$. Since all endomorphisms of $E_0 \otimes \overline{\mathbb{F}}_p$ are defined over $\mathbb{F}_{p^2}$, the group $\mathrm{Gal}(K/k)$ acts trivially on $G = \mathrm{Aut}(E_0 \otimes K)$.

By (4.1), the set $E(K/k, E_0 \otimes k)$ is in bijection with

$$H^1(\mathrm{Gal}(K/k), G) \simeq \mathrm{Hom}(\mathrm{Gal}(K/k), G)/G \simeq \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, G)/G, \quad (4.4)$$

where G acts $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, G)$ by conjugation. Note that the set $E(K/k, E_0 \otimes k)$ contains a non-trivial class.

Proposition 4.2. *Let $E_0/\mathbb{F}_{p^2}$, $m > 1$, $K = \mathbb{F}_{p^2}(T^{1/m})$ and $k = \mathbb{F}_{p^2}(T) \supset \mathbb{F}_{p^2}$ be above.*

(1) *Let E/k be an elliptic curve in a non-trivial class in $E(K/k, E_0 \otimes k)$. Then E is not k-isogenous to an elliptic curve E'/k which is defined over $\mathbb{F}_{p^2}$. In particular, E is not defined over $\mathbb{F}_{p^2}$.*

(2) *If $m = 3$ and $p = 2$, then $\mathrm{End}^0(E) \simeq \mathbb{Q}(\zeta_3)$, where ζ_n denotes a primitive nth root of unity.*

(3) *If $m = 2$ and p is odd, then $\mathrm{End}^0(E) \simeq B_{p,\infty}$.*

Proof.

(1) Suppose contrarily that there is an elliptic curve E_0' over $\mathbb{F}_{p^2}$ and a k-isogeny $\varphi : E_0' \otimes k \to E$. Choose a K-isomorphism $\alpha_K : E_0 \otimes_{\mathbb{F}_{p^2}} K \xrightarrow{\sim} E \otimes_k K$. We get a K-isogeny $\beta_K : E_0' \otimes_{\mathbb{F}_{p^2}} K \to E_0 \otimes_{\mathbb{F}_{p^2}} K$ such that $\varphi_K = \alpha_K \circ \beta_K$, where $\varphi_K = \varphi \otimes K$. Clearly $K/\mathbb{F}_{p^2}$ is primary, by

Lemma 3.2, β_K is defined over $\mathbb{F}_{p^2}$. As β_K and φ_K are defined over k, the isomorphism α_K is defined over k but E is not k-isomorphic to $E_0 \otimes_{\mathbb{F}_{p^2}} k$, a contradiction.

(2) Let $\{\xi\}$ be a 1-cocycle representing E, which can be viewed as an element in $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, G)$. Then $\xi_{\sigma_m} = \omega$, where $\omega \in G$ is an element of order 3. By Lemma 4.1 we have

$$\mathrm{End}^0(E) \simeq \{a \in \mathrm{End}^0(E_0 \otimes K) \mid \xi_\sigma \sigma(a) \xi_\sigma^{-1} = a,\ \forall\, \sigma \in \mathrm{Gal}(K/k)\}.$$

Therefore, $\mathrm{End}^0(E)$ is isomorphic to the centralizer of $\mathbb{Q}(\omega)$ in $B_{2,\infty}$ and $\mathrm{End}^0(E) = \mathbb{Q}(\omega)$.

(3) Using the same argument as (2), $\mathrm{End}^0(E)$ is isomorphic to the centralizer of $\mathbb{Q}$ in $B_{p,\infty}$ and hence $\mathrm{End}^0(E) \simeq B_{p,\infty}$. □

Proposition 4.3. *Let $g \geq 1$ be an integer, $\mathbb{F}$ a finite field of characteristic p and $k = \mathbb{F}(T)$, where T is a variable. Let A_0 be a g-dimensional abelian variety over $\mathbb{F}$. Then for any regular separable quadratic extension K/k, there exits a g-dimensional abelian variety A over k such that $A \otimes_k K$ is isomorphic to $A_0 \otimes_{\mathbb{F}} K$ but A is not k-isogenous to an abelian variety A' that is defined over a finite subfield of k.*

Proof. Since $K/\mathbb{F}$ is a primary extension, the Galois group $\mathrm{Gal}(K/k)$ acts trivially on $\mathrm{Aut}(A_0 \otimes_{\mathbb{F}} K)$. Thus, the set $E(K/k, A_0 \otimes_{\mathbb{F}} k) = \mathrm{Hom}(\mathrm{Gal}(K/k), \mathrm{Aut}(A_0 \otimes K))/\mathrm{Aut}(A_0 \otimes K)$ contains non-trivial classes. Let A be an abelian variety over k which is in a non-trivial class in $E(K/k, A_0 \otimes_{\mathbb{F}} k)$. The same proof as in Proposition 4.2 (1) shows that A satisfies the required properties. □

Theorem 1.2 (2) follows from Proposition 4.2 (1), or Proposition 4.3.

Remark 4.4.

(1) It follows from Proposition 4.2 that for any prime p, there exists an elliptic curve over k with smCM that is not k-isogenous to an elliptic curve which is defined over a finite field. This shows that the condition "up to a finite extension" in Grothendieck's theorem is necessary.

(2) It follows from Theorem 1.2 that there exists a superspecial abelian variety which is not defined over a finite field. Indeed, by Theorem 1.2 (2), there is a supersingular abelian variety A over some field k which

is not k-isogenous to an abelian variety A' which can be descended to a finite subfield of k. By Theorem 1.2 (1), let A_0 be a superspecial abelian variety over k which is k-isogenous to A, then A_0 is not defined over a finite field by the property of A. Proposition 4.3 exhibits examples of superspecial abelian varieties of any dimension which is not defined over a finite field.

5. Proof of Theorem 1.3

5.1. We need some fine arithmetic results of definite quaternion $\mathbb{Q}$-algebras; for example see [18, Proposition 3.1, p. 145]. Let $\mathfrak{A}$ be a definite quaternion $\mathbb{Q}$-algebra, $\mathcal{O}$ a maximal order in $\mathfrak{A}$ and $G = \mathcal{O}^\times$. Except for $\mathfrak{A} = B_{2,\infty}$ or $\mathfrak{A} = B_{3,\infty}$, the group G is cyclic of order $2, 4$ or 6.

When $\mathfrak{A} = B_{2,\infty} = (-1, -1/\mathbb{Q})$, the class number of $\mathcal{O}$ is one and any maximal order is conjugate to $\mathcal{O}$. Using the mass formula, $\#G = 24$. Furthermore, one has

$$G = E_{24} = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}.$$

When $\mathfrak{A} = B_{3,\infty} = (-1, -3/\mathbb{Q})$, the class number of $\mathcal{O}$ is one and any maximal order is conjugate to $\mathcal{O}$. Using the mass formula, $\#G = 12$. The group G is isomorphic to the binary dihedral group of order 12

$$G = T_{12} = \langle a, b \,|\, a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1} \rangle.$$

We also need some results arising from the inverse Galois problem. A useful result is that any finitely generated infinite field L over its prime field is *Hilbertian* (cf. [15, p. 298]), that is, the Hilbert irreducibility theorem for L holds. In particular the rational function field $\mathbb{F}_q(T)$ is Hilbertian.

5.2. Part (1): case $p = 2, 3$. Let $E_0/\mathbb{F}_{p^2}$ and $k = \mathbb{F}_{p^2}(T)$ be as in Section 4. Let $p = 2$ and $Q = \{\pm 1, \pm i, \pm j, \pm k\} \subset G := \mathrm{Aut}(E_0) = E_{24}$ the quaternion subgroup of order 8. We know that there is a generic Galois extension $L/k(s)$ with Galois group Q (see [5, Theorem 6.1.12, p. 140]), where s is a variable. By the Hilbert irreducibility theorem there is a finite Galois extension K/k with Galois group Q. Choose an isomorphism $\xi : \mathrm{Gal}(K/k) \xrightarrow{\sim} Q \subset G$ and

let $E \in E(K/k, E_0 \otimes k)$ be the member corresponding to the 1-cocycle $\{\xi_\sigma\}$ (noting that $\mathrm{Gal}(K/k)$ acts trivially on G). By the same computation as in Proposition 4.2, $\mathrm{End}^0(E)$ is isomorphic to the centralizer of Q in $B_{2,\infty}$. Clearly $\mathbb{Q}(Q) = B_{2,\infty}$ and $\mathrm{End}^0(E) = \mathbb{Q}$.

Now $p = 3$. Similarly using the Hilbert irreducibility theorem there is a finite Galois extension K/k with Galois group S_3; see [5, Remark, p. 29]. Choose an isomorphism $\xi : \mathrm{Gal}(K/k) \xrightarrow{\sim} S_3 \subset T_{12} = G$ and let $E \in E(K/k, E_0 \otimes k)$ be the member corresponding to the 1-cocycle $\{\xi_\sigma\}$. Using the same argument, $\mathrm{End}^0(E)$ is isomorphic to the centralizer of S_3 in $B_{3,\infty}$ and hence $\mathrm{End}^0(E) = \mathbb{Q}$.

5.3. Part (1): case $p > 3$. Since $p \not\equiv 1 \pmod{12}$, one has $p \equiv 3 \pmod 4$ or $p \equiv 2 \pmod 3$. Put $m = 4$ if $p \equiv 3 \pmod 4$ and $m = 6$ if $p \equiv 2 \pmod 3$ (choose any $m \in \{4, 6\}$ when $p \equiv 11 \pmod{12}$). There is a supersingular elliptic curve E_0 over $\mathbb{F}_p$ with $\mathrm{Aut}(E_0 \otimes \mathbb{F}_{p^2}) = C_m = \langle \eta \rangle$, where C_m is the cyclic group of order m and η is a generator. For example, let E_0 be the elliptic curve defined by $y^2 = x^3 - x$ or $y^2 = x^3 + 1$ for $p \equiv 3 \pmod 4$ or $p \equiv 2 \pmod 3$, respectively. Let $k = \mathbb{F}_p(T)$ and $\zeta_m \in \mathbb{F}_{p^2-1}^\times$ an element of order m. Note $m | p^2 - 1$ and $m \nmid p - 1$, thus $\zeta_m \notin \mathbb{F}_p^\times$ and $\mathbb{F}_{p^2} = \mathbb{F}_p[\zeta_m]$. Put $K = \mathbb{F}_{p^2}(T^{1/m})$ and $k_2 = \mathbb{F}_{p^2}(T)$. Then K/k is finite Galois with dihedral Galois group D_{2m} of order $2m$, which is generated by τ and c, where

$$c(\zeta_m) = \zeta_m^{-1}, \quad c(T^{1/m}) = T^{1/m}, \quad \tau(T^{1/m}) = \zeta_m T^{1/m}, \quad \tau \in \mathrm{Gal}(K/k_2).$$

We may identify $\mathrm{Gal}(k_2/k) = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \{1, c\}$ and c acts on $\mathrm{Aut}(E_0 \otimes \mathbb{F}_{p^2})$ by $c(\eta) = \eta^{-1}$.

Define a 1-cocycle $\{\xi_\sigma\} \in Z^1(\mathrm{Gal}(K/k), C_m)$ by

$$\xi_{\tau^i} = \eta^i, \quad \xi_{c\tau^i} = \eta^{-i} d, \quad \forall\, i = 0, \ldots, m-1,$$

where d is any element in C_m, and let E be the corresponding elliptic curve over $k = \mathbb{F}_p(T)$. Then

$$\mathrm{End}^0(E) \simeq \{a \in \mathrm{End}^0(E_0 \otimes K) \,|\, \xi_\sigma \sigma(a) \xi_\sigma^{-1} = a, \ \forall\, \sigma \in \mathrm{Gal}(K/k)\}.$$

Let $a \in \mathrm{End}^0(E)$ be an element. Put $\sigma = \tau$, then one has $a \in \mathbb{Q}(\eta)$. Put $\sigma = c$, then $c(a) = a$ implies $a \in \mathbb{Q}$. Thus, $\mathrm{End}^0(E) = \mathbb{Q}$.

5.4. Part (2). Theorem 1.3 (2) will follow from the following two lemmas.

Lemma 5.1. *If $p > 3$ and the base field k contains $\mathbb{F}_{p^2}$, then the endomorphism algebra of any supersingular elliptic curve E over k is isomorphic to either $B_{p,\infty}$, $\mathbb{Q}(\zeta_4)$, or $\mathbb{Q}(\zeta_6)$. In particular,* $\mathrm{End}^0(E) \neq \mathbb{Q}$.

Proof. We know that any supersingular j-invariant is contained $\mathbb{F}_{p^2}$ and that any elliptic curve E' over an algebraically closed field of characteristic p has a model defined over $\mathbb{F}_p(j)$. There is a finite Galois extension K/k, a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$ and a K-isomorphism $E \otimes K \simeq E_0 \otimes_{\mathbb{F}_{p^2}} K$, that is E is a K/k-form of $E_0 \otimes k$. Replacing E_0 by a form of itself and increasing K if necessarily we may assume that $\mathrm{End}^0(E_0) \simeq B_{p,\infty}$. Since all $\overline{\mathbb{F}}_p$-endomorphisms of $E \otimes \overline{\mathbb{F}}_p$ is defined over $\mathbb{F}_{p^2}$, the group $\mathrm{Gal}(K/k)$ acts trivially on $\mathrm{End}(E_0 \otimes K)$. As $p > 3$, the automorphism group $G = \mathrm{Aut}(E_0)$ is abelian and $H^1(\mathrm{Gal}(K/k), G) \simeq \mathrm{Hom}(\mathrm{Gal}(K/k), G)$. Let $\xi \in \mathrm{Hom}(\mathrm{Gal}(K/k), G)$ be the 1-cocycle corresponding to E. Similarly, $\mathrm{End}^0(E)$ is isomorphic to the centralizer of the image of ξ. It follows that $\mathrm{End}^0(E) \simeq B_{p,\infty}$ or $\mathbb{Q}(\zeta_m)$ according as $\mathrm{Im}(\xi) \subset \{\pm 1\}$ or $\mathrm{Im}(\xi) = C_m$ with $m = 4, 6$. □

Lemma 5.2. *Assume that $p \equiv 1 \pmod{12}$ and $k \not\supset \mathbb{F}_{p^2}$. Then for any supersingular elliptic curve E over k, one has* $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{-p})$.

Proof. Replacing k by a subfield of itself we may assume that k is finitely generated over $\mathbb{F}_p$. The algebraic closure $\mathbb{F}_q$ of $\mathbb{F}_p$ in k has cardinality $q = p^a$ of an odd power of p.

Since $j(E) \in \mathbb{F}_q \cap \mathbb{F}_{p^2} = \mathbb{F}_p$, there is a supersingular elliptic curve E_0 over $\mathbb{F}_p$, a finite Galois extension K/k, and a K-isomorphism $E \otimes K \simeq E_0 \otimes K$ (see the proof of Lemma 5.1). Particularly E is a K/k-form of $E_0 \otimes k$. The Frobenius endomorphism π_{E_0} of E_0 satisfies $\pi_{E_0}^2 = -p$ as $p > 3$. Since the Frobenius endomorphism of $E_0 \otimes \mathbb{F}_q$ is not in $\mathbb{Q}$, one has $\mathrm{End}^0(E_0 \otimes \mathbb{F}_q) = \mathbb{Q}(\pi_{E_0}^a) = \mathbb{Q}(\sqrt{-p})$. By Lemma 3.2, $\mathrm{End}^0(E_0 \otimes k) = \mathrm{End}^0(E_0 \otimes \mathbb{F}_q) = \mathbb{Q}(\sqrt{-p})$. Our assumption of p implies that $\mathrm{Aut}(E_0 \otimes K) = \{\pm 1\}$ (see [3, Table 1.3, p. 117]), which is contained in the center of $\mathrm{End}(E_0 \otimes K)$. Finally by Lemma 4.1 one has

$$\begin{aligned} \mathrm{End}^0(E) &\simeq \{a \in \mathrm{End}^0(E_0 \otimes K) \mid \sigma(a) = a,\ \forall \sigma \in \mathrm{Gal}(K/k)\} \qquad (5.1) \\ &= \mathrm{End}^0(E_0 \otimes k) \simeq \mathbb{Q}(\sqrt{-p}). \end{aligned}$$

□

For the convenience of the reader, we make the following table of isogeny classes and endomorphism algebras of supersingular elliptic curves over finite fields (cf. [19, Chapter 4]). Here E denotes a supersingular elliptic curve over $\mathbb{F}_q$, $q = p^a$, $\zeta_n := \exp(2\pi i/n) \in \mathbb{C}$ and π is the Frobenius endomorphism of E, which is represented by a Weil q-number.

	a is even		
π	$\pm p^{a/2}$	$p^{a/2}\zeta_4$, $p \not\equiv 1 \pmod 4$	$\pm p^{a/2}\zeta_6, p \not\equiv 1 \pmod 3$
$\mathrm{End}^0(E)$	$B_{p,\infty}$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$
	a is odd		
π	$\sqrt{q}\zeta_4$	$\pm\sqrt{2^a}\zeta_8$	$\pm\sqrt{3^a}\zeta_{12}$
$\mathrm{End}^0(E)$	$\mathbb{Q}(\sqrt{-p})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$

5.5. We discuss endomorphism algebras of ordinary elliptic curves over any field of characteristic p, for the sake of completeness. No new algebra appears in this case.

Lemma 5.3. *Let E be an ordinary elliptic curve over a field k. Then $\mathrm{End}^0(E)$ is either $\mathbb{Q}$ or an imaginary quadratic field over which p splits.*

Proof. It is well known that $\mathrm{End}^0(E_{\bar{k}})$ is either $\mathbb{Q}$ or an imaginary quadratic field for which p splits, and hence so is $\mathrm{End}^0(E)$. □

6. Higher Dimensional Examples

We give two new examples of endomorphism algebras of supersingular abelian varieties of higher dimensional.

Theorem 6.1. *For every positive integer d and every prime $p \not\equiv 1 \pmod{12}$ there exists a supersingular abelian variety A of dimension d over a field k of characteristic p such that $\mathrm{End}^0(A) = \mathbb{Q}$.*

Proof. Since $p \not\equiv 1 \pmod{12}$, there exits a supersingular elliptic curve E over $k = \mathbb{F}_q(T)$ for some finite field $\mathbb{F}_q$ of q elements such that $\mathrm{End}^0(E) = \mathbb{Q}$ by Theorem 1.3 (1). Let k'/k be a finite separable field extension such that $\mathrm{End}^0(E_{\bar{k}}) = \mathrm{End}^0(E_{k'}) = B_{p,\infty}$. Since k is Hilbertian, there exists a finite Galois extension K/k linearly disjoint from k' over k such that $\mathrm{Gal}(K/k) \simeq S_{d+1}$, the symmetric group of $d+1$ letters. Put $A' := E^d$. As $\mathrm{End}(E_K) =$

$\mathrm{End}(E) = \mathbb{Z}$, one has $\mathrm{Aut}(A'_K) = \mathrm{Aut}(A') = \mathrm{GL}_d(\mathbb{Z})$ and the Galois group $\mathrm{Gal}(K/k)$ acts trivially on this group.

Let S_{d+1} operate by permutation on the vector space $\mathbb{Q}^{d+1}$. One has the decomposition $\mathbb{Q}^{d+1} = \mathbb{Q} \oplus V$ of two absolutely irreducible representations. Choosing a suitable basis of V, one obtains a map $\rho : S_{d+1} \to \mathrm{GL}_d(\mathbb{Z})$ such that the centralizer of $\rho(S_{d+1})$ in $M_d(\mathbb{Q})$ is $\mathbb{Q}$. Since $\mathrm{Gal}(K/k)$ acts trivially on $\mathrm{Aut}(A'_K) = \mathrm{GL}_d(\mathbb{Z})$, the map ρ defines a 1-cycle in $Z^1(\mathrm{Gal}(K/k),$ $\mathrm{Aut}(A'_K)) = \mathrm{Hom}(\mathrm{Gal}(K/k), \mathrm{Aut}(A'_K))$ which corresponds to a supersingular abelian variety A over k by Galois descent. By Lemma 4.1, the endomorphism algebra of A over k is equal to the centralizer of $\rho(S_{d+1})$ in $M_d(\mathbb{Q})$, which is $\mathbb{Q}$ by our construction. □

Theorem 6.2. *For every positive integer d and every prime $p \not\equiv 1 \pmod{24}$ there exists a supersingular abelian variety A of dimension $2d$ over a field k of characteristic p such that the endomorphism algebra $\mathrm{End}^0(A)$ of A is isomorphic to $F := \mathbb{Q}(\sqrt{p})$.*

Proof. Since $p \not\equiv 1 \pmod{24}$, by [8, Proposition 9.4] there exists a supersingular abelian surface X over $k = \mathbb{F}_{p^{2^\infty}}(T)$, where $\mathbb{F}_{p^{2^\infty}} = \cup_n \mathbb{F}_{p^{2^n}}$, such that $\mathrm{End}^0(X) = \mathbb{Q}(\sqrt{p})$. By [24, Theorem 1.3], we may assume that $\mathrm{End}(X)$ is the ring of integers O_F of F. Since k is Hilbertian, similar to the proof of Theorem 6.1, there exists a finite Galois extension K/k with group S_{d+1} such that $\mathrm{End}(X_K) = \mathrm{End}(X) = O_F$. Put $A' := X^d$ and then $\mathrm{Gal}(K/k)$ acts trivially on $\mathrm{Aut}(A'_K) = \mathrm{Aut}(A') = \mathrm{GL}_d(O_F)$.

Similar to Theorem 6.1, one obtains a map $\rho : S_{d+1} \to \mathrm{GL}_d(\mathbb{Z}) \subset \mathrm{GL}_d(O_F)$ such that the centralizer of $\rho(S_{d+1})$ in $M_d(\mathbb{Q}) = \mathrm{End}(V)$ is $\mathbb{Q}$. Since V is absolutely irreducible, the centralizer of $\rho(S_{d+1})$ in $M_d(F)$ is F. The group homomorphism ρ defines a 1-cycle in $Z^1(\mathrm{Gal}(K/k), \mathrm{Aut}(A'_K))$ and it corresponds to a supersingular abelian variety A over k of dimension $2d$. It is then easy to see that the endomorphism algebra of A over k is equal to the centralizer of $\rho(S_{d+1})$ in $M_d(F)$, which is F. □

Erratum to [23]

Very unfortunately the main result Theorem 1.2 in [23] is not correct as stated. We apologize to the Journal for overlooks. Theorem 1.1 is an equivalent statement of Theorem 1.2. Our purpose of formulating this theorem

was to introduce invariants which could control the finiteness. However, this approach turns out not working well. The errors occur at the proofs of two reduction steps Lemmas 2.2 and 2.4, loc.cit.

To see that the second assertion (2.2) of Lemma 2.2 is false, take a supersingular elliptic curve E over $\mathbb{F}_7$ whose endomorphism ring is $\mathbb{Z}[\sqrt{-7}]$, which has index 2 in the maximal order. However, the endomorphism ring of $E \otimes \mathbb{F}_{p^2}$ is a maximal order of the quaternion algebra over $\mathbb{Q}$ ramified at $\{7, \infty\}$.

To correct (2.2) of Lemma 2.2 one should impose an additional condition that $\mathrm{End}(A)$ is contained in the center of $\mathrm{End}(A_{k'})$, where $A_{k'} = A \otimes_k k'$.

Proof. Since $\mathrm{End}(A \otimes k^{\mathrm{perf}}) = \mathrm{End}(A)$, where k^{perf} is the perfect closure of k, we may assume that both k and k' are perfect by replacing them by their perfect closure. Choose a maximal order O_1 in the endomorphism algebra $\mathrm{End}^0(A)$ containing $\mathrm{End}(A)$. Let $M \subset M'$ be the Dieudonné modules of A and $A_{k'}$, respectively. Put $M_1 := O_1 M$ and let $A \to A_1$ be the isogeny (unique up to isomorphism) realizing $M \to M_1$. Write $\alpha : \mathrm{End}^0(A) \xrightarrow{\sim} \mathrm{End}^0(A_1)$ for the isomorphism. Then $\alpha(O_1) = \mathrm{End}(A_1)$ and it is contained in $\mathrm{End}(A_{1k'})$. Now from our assumption that O_1 commutes with $\mathrm{End}(A_{k'})$, the latter leaves the Dieudonné module $M_1' := M(A_1 \otimes k') = O_1 M'$ stable. This shows that $\alpha(\mathrm{End}(A_{k'})) \subset \mathrm{End}(A_{1k'})$. An element $x \in O_{1p} = O_1 \otimes \mathbb{Z}_p$ lies in O_p if and only if $xM \subset M$, or the same $xM' \subset M'$. Thus, $\alpha(O_{1p}) \cap \alpha(\mathrm{End}(A_{k'}) \otimes \mathbb{Z}_p) = \alpha(\mathrm{End}(A) \otimes \mathbb{Z}_p)$ and we have an injective map

$$\alpha : \frac{O_{1p}}{\mathrm{End}(A) \otimes \mathbb{Z}_p} \to \frac{\mathrm{End}(A_{1k'}) \otimes \mathbb{Z}_p}{\alpha(\mathrm{End}(A_{k'}) \otimes \mathbb{Z}_p)}.$$

Using the Tate modules instead of Dieudonné modules, we get an injective map

$$\alpha : \frac{O_1}{\mathrm{End}(A)} \to \frac{\mathrm{End}(A_{1k'})}{\alpha(\mathrm{End}(A_{k'}))}. \qquad \square$$

The statement of Lemma 2.4 should be corrected by imposing an additional condition that $\mathrm{End}(A) \otimes \mathbb{Z}_p$ is contained in the center of $\mathrm{End}(A[p^\infty])$. This condition ensures that $\mathrm{End}(A[p^\infty])$ is contained in $\mathrm{End}(A'[p^\infty])$ in the proof of Lemma 2.4.

Our fixes of Lemmas 2.2 and 2.4 point out what should be correct, but do not save Theorem 1.2 as it is not correct due to the following counterexample.

Counterexample to Theorem 1.2. Choose a simple ordinary abelian surface A_0 over $\overline{\mathbb{F}}_p$. Modifying A_0 by an isogeny, we can assume that its endomorphism ring $O := \mathrm{End}(A_0)$ is the maximal order in a CM field $K := \mathrm{End}^0(A_0)$ [24, Theorem 1.3]. Let M_0 be the Dieudonné module of A_0, and let $M_0 = M_0^0 \oplus M_0^1$ be the isotypic decomposition with slopes 0 and 1, respectively. The endomorphism ring $\mathrm{End}(M_0) = \mathrm{End}(M_0^0) \times \mathrm{End}(M_0^1)$ also decomposes. We fix a $\mathbb{Z}_p$-basis for the skeleton of each M_0^i ([23, (3.4), p. 363]) and have $\mathrm{End}(M_0^i) = \mathrm{Mat}_2(\mathbb{Z}_p)$. The action of the order $O_p := O \otimes \mathbb{Z}_p$ leaves each component M_0^i invariant. As O is the maximal order in K, one has $O_p = O_p^0 \times O_p^1$ and $O_p^i \subset \mathrm{End}(M_0^i)$ for $i = 1, 2$. Consider a Dieudonné submodule $M_1 = M_1^0 \oplus M_1^1 \subset M_0$ with $M_1^1 = M_0^1$, and let $A_1 \to A_0$ be the isogeny realizing the inclusion $M_1 \subset M_0$. Since M_1^0 is isomorphic to M_0^0, it is of the form gM_0^0, where $g \in \mathrm{Aut}(M_0^0[1/p]) = \mathrm{GL}_2(\mathbb{Q}_p)$. Note $\mathrm{End}(A_1)$ is contained in O as O is the unique maximal order in K. Therefore, $\mathrm{End}(A_1) \otimes \mathbb{Z}_p = O_{1p}^0 \times O_p^1$ with $O_{1p}^0 = O_p^0 \cap g\mathrm{End}(M_0^0)g^{-1} = O_p^0 \cap g\mathrm{Mat}_2(\mathbb{Z}_p)g^{-1}$. Thus,

$$[O_p : \mathrm{End}(A_1) \otimes \mathbb{Z}_p] = [O_p^0 : O_p^0 \cap g\mathrm{Mat}_2(\mathbb{Z}_p)g^{-1}].$$

This index is unbounded for all $g \in \mathrm{GL}_2(\mathbb{Q}_p)$.

Lemma *Let A be an abelian variety over a perfect field k, and let $A \to A^{\min}$ be its minimal isogeny. Let $M \subset M_0$ be the Dieudonné modules of this isogeny and put $\overline{M} := M \otimes_W W(\bar{k})$ and $\overline{M}_0 := M_0 \otimes_W W(\bar{k})$. Let*

$$O := \mathrm{End}(A), \quad \Lambda := \mathrm{End}(M), \quad \overline{\Lambda} := \mathrm{End}(\overline{M}),$$

$$O_0 := \mathrm{End}(A^{\min}), \quad \Lambda_0 := \mathrm{End}(M_0), \quad \overline{\Lambda}_0 := \mathrm{End}(\overline{M}_0).$$

Then we have inclusions

$$\frac{O_0}{O} = \frac{O_0 \otimes \mathbb{Z}_p}{O \otimes \mathbb{Z}_p} \subset \frac{\Lambda_0}{\Lambda} \subset \frac{\overline{\Lambda}_0}{\overline{\Lambda}}.$$

Proof. By Lemma 2.4 of this note, the minimal Dieudonné module M_0 is generated by M and certain operators only involving powers of F, V, p.

As elements of $\mathrm{End}(M)$ commute with these operators, one has $\mathrm{End}(M) \subset \mathrm{End}(M_0)$ and $O \subset O_0$, and hence $\mathrm{End}(\overline{M}) \subset \mathrm{End}(\overline{M}_0)$. Now the lemma follows from $O_0 \cap \mathrm{End}(M) = O$ and $\Lambda_0 \cap \mathrm{End}(\overline{M}) = \mathrm{End}(M)$. □

For any field k and integer $g \geq 1$, denote by $\mathcal{A}_g^{un}(k)$ the set of isomorphism classes of g-dimensional abelian varieties over k.

Corollary *Let k be any field of characteristic p and $g \geq 1$ a fixed integer. Let $\mathcal{B} \subset \mathcal{A}_g^{un}(k)$ be a subset which is stable under isogeny. Then the following two statements are equivalent.*

(a) *There are only finitely many isomorphism classes of $\mathbb{Z}_p$-orders $\mathrm{End}(A) \otimes \mathbb{Z}_p$ for all abelian varieties $A \in \mathcal{B}$.*

(b) *There are only finitely many isomorphism classes of $\mathbb{Z}_p$-orders $\mathrm{End}(A) \otimes \mathbb{Z}_p$ for all minimal abelian varieties $A \in \mathcal{B}$.*

Proof. Again we may assume that k is perfect as $\mathrm{End}(A_{k^{\mathrm{perf}}}) = \mathrm{End}(A)$ and A is minimal if and only if so is $A_{k^{\mathrm{perf}}}$. By [23, Theorem 2.5], $|\overline{\Lambda}_0/\overline{\Lambda}| \leq p^N$ for an integer N which depends only on g. Then the corollary follows from *Lemma*. □

We change Theorem 1.2 into the following weaker result, which suffices to imply Corollary 1.3 and Theorem 1.4 (Deuring) in [23]. See [1, Definition 2.1] for the definition of hypersymmetric abelian varieties.

Theorem *Notations as in Corollary, let $\mathcal{I} \subset \mathcal{A}_g^{un}(k)$ be one isogeny class. There are only finitely many isomorphism classes of $\mathbb{Z}_p$-orders $\mathrm{End}(A) \otimes \mathbb{Z}_p$ for all abelian varieties $A \in \mathcal{I}$ provided one of the following conditions holds:*

(a) *There are only finitely many isomorphism classes of $\mathbb{Z}_p$-orders $\mathrm{End}(A) \otimes \mathbb{Z}_p$ for all minimal abelian varieties $A \in \mathcal{I}$.*

(b) *The field k is algebraically closed and any member A in $\mathcal{I}$ is hypersymmetric.*

Condition (b) implies condition (a). It is natural to ask whether or not an abelian variety over an algebraically closed field k whose isogeny class satisfies condition (a) in *Theorem* is hypersymmetric.

Acknowledgments

The author is grateful to Ching-Li Chai and Akio Tamagawa for helpful discussions. The present work is done during the author's stay in the Max-Planck-Institut für Mathematik. He is grateful to the Institut for kind hospitality and excellent working environment. The author was partially supported by the grants MoST 100-2628-M-001-006-MY4 and 103-2918-I-001-009. He thanks the referee for a careful reading and helpful comments.

References

1. C.-L. Chai and F. Oort, Hypersymmetric abelian varieties, *Pure Appl. Math. Q.*, **2** (2006), 1-27.

2. Ching-Li Chai, Brian Conrad and Frans Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, **195**. AMS, 387 pp.

3. B. H. Gross, Heights and the special values of L-series. Number theory (Montreal, Que., 1985), 115-187, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.

4. S. Harashita, On p-divisible groups with saturated Newton polygons, *Nagoya Math. J.*, **232** (2018), 96-120.

5. Christian U. Jensen, Arne Ledet and Noriko Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, **45**. Cambridge University Press, 2002. 258 pp.

6. N. M. Katz, Slope filtration of F-crystals, *Journées de Géométrie. Algébrique de Rennes*, **I** (1978), 113-163, Astérisque, 63. Soc. Math. France, Paris, 1979.

7. K.-Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties,* Lecture Notes in Math., vol. 1680, Springer-Verlag, 1998.

8. Qun Li, Jiangwei Xue and C.-F. Yu, Unit groups of maximal orders in totally definite definite quaternion algebras over real quadratic fields, arXiv:1807.04736v2, 54 pp. To appear in *Trans. Amer. Math. Soc.*

9. Yu. Manin, Theory of commutative formal groups over fields of finite characteristic, *Russian Math. Surveys*, **18** (1963), 1-80.

10. D. Mumford, *Abelian Varieties*, Oxford University Press, 1974.

11. F. Oort, The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field, *J. Pure Appl. Algebra*, **3** (1973), 399-408.

12. F. Oort, Subvarieties of moduli spaces, *Invent. Math.*, **24** (1974), 95-119.

13. F. Oort, Which abelian surfaces are products of elliptic curves? *Math. Ann.*, **214** (1975), 35-47.

14. F. Oort and T. Zink, Families of p-divisible groups with constant Newton polygon, *Doc. Math.*, **7** (2002), 183-201.

15. A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications 77. Cambridge University Press, 2000. 558 pp.

16. J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.*, **2** (1966), 134-144.

17. J. Tate, Classes d'isogenie de variétés abéliennes sur un corps fini (d'après T. Honda). *Sém. Bourbaki Exp.* 352 (1968/69), Lecture Notes in Math., vol. 179, Springer-Verlag, 1971.

18. M.-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Math., vol. 800, Springer-Verlag, 1980.

19. W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* (4), **2** (1969), 521-560.

20. A. Weil, The field of definition of a variety, *Amer. J. Math.*, **78** (1956), 509-524.

21. J. Xue, T.-C. Yang and C.-F. Yu, On superspecial abelian surfaces over finite fields, *Doc. Math.*, **21** (2016), 1607-1643.

22. C.-F. Yu, The isomorphism classes of abelian varieties of CM-type, *J. Pure Appl. Algebra*, **187** (2004), 305-319.

23. C.-F. Yu, On finiteness of endomorphism rings of abelian varieties, *Math. Res. Lett.*, **17** (2010), no. 2, 357-370.

24. C.-F. Yu, On the existence of maximal orders, *Int. J. Number Theory*, **7** (2011), no. 8, 2091-2114.

25. C.-F. Yu, Endomorphism algebras of QM abelian surfaces, *J. Pure Appl. Algebra*, **217** (2013), 907-914.

26. Th. Zink, On the slope filtration, *Duke Math. J.*, **109** (2001), 79-95.

27. Th. Zink, *Cartiertheorie kommutativer formaler Gruppen*, Teubner-Texte Math. Teubner, Leipzig, 1984.