A NOTE ON SUPERSINGULAR ABELIAN VARIETIES

CHIA-FU YU

Abstract. It is shown that any supersingular abelian variety is isogenous to a superspecial abelian variety without increasing field extensions. We construct superspecial abelian varieties which are not defined over finite fields. Endomorphism algebras of supersingular elliptic curves over an arbitrary field are also investigated.

1. Introduction

Let p be a prime number. In this note we discuss endomorphism algebras and fields of definition for isogenies of abelian varieties in characteristic p. Let k denote a field of characteristic p and $\bar{k}$ an algebraic closure of k. Recall that an elliptic curve over k is supersingular if it has no non-zero $\bar{k}$-valued p-torsion points. An abelian variety over k is *supersingular* if it is isogenous over a product of supersingular elliptic curves over $\bar{k}$; it is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over $\bar{k}$. The following well-known result due to Deligne, Shioda and Ogus (cf. [4, Section 1.6, p. 13]) is important for studying supersingular abelian varieties.

Theorem 1.1. *For any integer $g \geq 2$, there is only one isomorphism class of g-dimensional superspecial abelian varieties over $\bar{k}$.*

Particularly any g-dimensional superspecial abelian variety over $\bar{k}$ is defined over $\mathbb{F}_p$ if $g > 1$ (and over $\mathbb{F}_{p^2}$ if $g = 1$ due to Deuring). For convenience of discussion, we say an abelian variety A over k *trained* if there is an abelian variety A_0 over a finite field $k_0 \subset k$ and a k-isomorphism $A_0 \otimes k \simeq A$. Do not confuse this with the weaker property that the field of moduli of A is a finite field.

Consider the following two statements:

(A) Any supersingular abelian variety over k is isogenous to a superspecial abelian variety over k (without increasing a field extension).

(B) Any superspecial abelian variety is trained.

A main result of this note shows the following.

Theorem 1.2. *Statement (A) holds.*

It is well known that not every supersingular abelian variety over k or even over $\bar{k}$ is trained. Theorems 1.1 and 1.2 suggest that Statement (B) is false in general. Otherwise every supersingular abelian variety would be isogenous to a product of supersingular elliptic curves over the same ground field. We confirm

Date: December 25, 2014.

2010 *Mathematics Subject Classification.* 14K15, 11G10.

Key words and phrases. supersingular abelian varieties, Galois descent.

this by constructing counterexamples to Statement (B) (Section 3). This answers negatively to a question in [14, (Q), p. 912]. Our construction relies on some fine arithmetic properties of definite quaternion $\mathbb{Q}$-algebras and an explicit computation of Galois cohomology.

A related topic is a theorem of Grothendieck, which states that if A is an abelian variety with smCM over a field $k \supset \mathbb{F}_p$, 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 $\varphi : A \otimes_k k_1 \sim A_0 \otimes_{k_0} k_1$; see [5, pp. 220/221], [6, Theorem 1.1] and [13, Theorem 1.4]. An abelian variety A is said to have *smCM* if its endomorphism algebra $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ contains a commutative semi-simple $\mathbb{Q}$-subalgebra of degree $2 \dim A$. The conditions "up to isogeny" and "up to a finite extension" in Grothendieck's theorem are necessary. For example, a geometric generic supersingular abelian surface is not defined over a finite field. Our counterexamples to Statement (B) also show that the condition "up to a finite extension" is necessary.

Galois descent and Theorem 1.1 play important roles in the proof of Statement (A). The theory also allows us to compute the endomorphism algebras of abelian varieties twisted by 1-cocycles, not just classifying them. This leads to the following result about endomorphism algebras of supersingular elliptic curves, over an arbitrary field of characteristic p. It differs sightly from well-known results where k is a finite field that $\mathbb{Q}$ also occurs in the endomorphism algebras in question.

Let $B_{p,\infty}$ denote the (unique up to isomorphism) quaternion $\mathbb{Q}$-algebra ramified exactly at $\{p, \infty\}$.

Theorem 1.3.

(1) *If* $p \not\equiv 1 \pmod{12}$, *then there is a supersingular elliptic curve* E *over a field* k *of characteristic* p *so 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 *of characteristic* p, *one has* $\mathrm{End}^0(E) \neq \mathbb{Q}$; *i.e.* $\mathrm{End}^0(E)$ *is a semi-simple* $\mathbb{Q}$*-subalgebra of degree* 2 *or* 4 *in* $B_{p,\infty}$.

The proof of Theorem 1.3 (1) is given by an explicit construction, which depends on a construction of some Galois field extensions. The involved inverse Galois problem (IGP) is fortunately rather easy to solve.

Our proof of Theorem 1.3 (2) also gives all possible $\mathbb{Q}$-algebras that can occur as the endomorphism algebras of supesingular elliptic curves. However, all of them, no matter these curves are trained or not, occur in the endomorphism algebras of those over finite fields.

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. [10, 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	$\pm p^{a/2}$	$p^{a/2}\zeta_4$, $p \equiv 3 \pmod 4$	$\pm p^{a/2}\zeta_6, p \equiv 2 \pmod 3$
$\mathrm{End}^0(E)$	$B_{p,\infty}$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$

	a is odd		
π	$\sqrt{q}\zeta_4$	$\pm\sqrt{2^a}\zeta_8$	$\pm\sqrt{3^a}\zeta_{12}$
$\mathrm{End}^0(E)$	$\mathbb{Q}(\sqrt{-p})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$

2. Proof of Statement (A)

We will prove the following result.

Proposition 2.1. *Let A be a supersingular abelian variety over a field k of characteristic p. There exists a superspecial abelian variety C over k and a k-isogeny $A \to C$.*

Lemma 2.2. *Let A be as in Proposition 2.1. 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. This is a known fact; a proof is provided for the reader's convenience. 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. Let M be the covariant Dieudonné module of A. It is known that 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 2.3. *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 the isomorphism*

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

Proof. See [1, 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. ∎

We briefly recall the theory of Galois descent. Let K/k be a finite Galois extension and $\mathrm{Gal}(K/k)$ the Galois group. Let X_0 be a quasi-projective variety over k. Suppose X is a quasi-projective variety over K and $f : X_0 \otimes_k K \xrightarrow{\sim} X$ is a K-isomorphism. For any elements $\sigma, \tau \in \mathrm{Gal}(K/k)$, define $f_{\tau,\sigma} = \tau(f) \circ \sigma(f)^{-1} : {}^\sigma X \xrightarrow{\sim} {}^\tau X$ so that the following diagram commutes

$$\begin{array}{ccc} X_0 \otimes_k K & \xrightarrow{\sigma(f)} & {}^\sigma X \\ \downarrow{=} & & \downarrow{f_{\tau,\sigma}} \\ X_0 \otimes_k K & \xrightarrow{\tau(f)} & {}^\tau X. \end{array}$$

Clearly the relation $f_{\sigma_1,\sigma_2} \circ f_{\sigma_2,\sigma_3} = f_{\sigma_1,\sigma_3}$ holds for any $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Gal}(K/k)$. If we put

$$a_\sigma := f_{\sigma,1} = \sigma(f) \circ f^{-1} : X \xrightarrow{\sim} {}^\sigma X$$

then we have

$$a_{\sigma\tau} = \sigma(a_\tau) \circ a_\sigma : X \xrightarrow{a_\sigma} {}^\sigma X \xrightarrow{\sigma(a_\tau)} {}^{\sigma\tau} X,$$

i.e. $\{a_\sigma\}$ forms a 1-cocycle.

Weil's theorem on Galois descent [11] says that if Y is a quasi-projective variety over K, and for any $\sigma \in \mathrm{Gal}(K/k)$, there is an isomorphism $a_\sigma : Y \xrightarrow{\sim} {}^\sigma Y$

satisfying the 1-cocycle condition, then there is a variety Y_0' (necessarily quasi-projective) over k and a K-isomorphism $\eta : Y_0'\otimes K \simeq Y$ such that $a_\sigma = \sigma(\eta)\circ\eta^{-1}$ for all $\sigma\in \mathrm{Gal}(K/k)$.

Suppose that $X = X_0 \otimes K$ for a quasi-projective variety X_0 over k. Then for any 1-cocycle $\{\xi_\sigma\}_{\sigma\in\mathrm{Gal}(K/k)} \in Z^1(\mathrm{Gal}(K/k), \mathrm{Aut}(X))$, there is a quasi-projective variety X_0' over k and a K-isomorphism $\eta : X_0'\otimes K \xrightarrow{\sim} X$ such that $\xi_\sigma = \sigma(\eta)\eta^{-1}$ for all $\sigma \in \mathrm{Gal}(K/k)$. The construction from $\{\xi_\sigma\}$ to X_o' induces a bijection between the Galois cohomology $H^1(\mathrm{Gal}(K/k), \mathrm{Aut}(X))$ and the set $E(K/k, X_0)$ of k-isomorphism classes of K/k-forms of X_0.

Let $\mathrm{End}(X_0')$ (resp. $\mathrm{End}(X_0'\otimes K)$) denote the monoid of endomorphisms $f : X_0' \to X_0'$ over k (resp. $f : X_0'\otimes K \to X_0'\otimes K$ over K). The isomorphism η above induces an isomorphism $\alpha : \mathrm{End}(X_0'\otimes K) \to \mathrm{End}(X)$ by $\alpha(a) := \eta a\eta^{-1}$, i.e. the following diagram commutes

$$\begin{array}{ccc} X_o'\otimes K & \xrightarrow{\ \eta\ } & X \\ \Big\downarrow{\scriptstyle a} & & \Big\downarrow{\scriptstyle \alpha(a)} \\ X_o'\otimes K & \xrightarrow{\ \eta\ } & X. \end{array}$$

We express $\sigma(\alpha(a))$ in terms of $\alpha(a)$ as follows

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

Thus, $\alpha(\sigma(a)) = \xi_\sigma^{-1}\cdot\sigma(\alpha(a))\cdot\xi_\sigma$. In other words, if α sends an element a to a', then it sends the element $\sigma(a)$ to $\xi_\sigma^{-1}\cdot\sigma(a')\cdot\xi_\sigma$. Therefore, the map α induces the following isomorphism

$$\begin{aligned} \mathrm{End}(X_0') &= \{a\in \mathrm{End}(X_0'\otimes K) \mid \sigma(a) = a, \forall\,\sigma\in\mathrm{Gal}(K/k)\} \\ &\xrightarrow{\sim} \{a'\in\mathrm{End}(X) \mid \xi_\sigma^{-1}\sigma(a')\xi_\sigma = a', \forall\,\sigma\in\mathrm{Gal}(K/k)\}. \end{aligned} \tag{2.1}$$

We now can show the following key lemma.

Lemma 2.4. *Let L/k be a finite purely inseparable extension field and B a superspecial abelian variety B over L of dimension $g\ge 2$. 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 2.3 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_s 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_s is a purely inseparable field extension of degree $[L:k]$, L and k_s are linearly disjoint over k, and the restriction gives an isomorphism $\mathrm{Gal}(K/L)\simeq\mathrm{Gal}(k_s/k)$. Identifying $\mathrm{Gal}(K/L)$ with $\mathrm{Gal}(k_s/k)$, and $\mathrm{Aut}(A_K)$ with $\mathrm{Aut}(A_{k_s})$ due to Lemma 2.3, we regard $\{\xi_\sigma\}$ as a 1-cocycle of $\mathrm{Gal}(k_s/k)$ with values in $\mathrm{Aut}(A_{k_s})$. 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 Proposition 2.1 There is nothing to prove if $g = \dim(A) = 1$; we may assume that $g \geq 2$. By Lemma 2.2, 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 2.4 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 2.3 φ is defined over k. ∎

3. Counterexamples to Statement (B)

3.1. We shall construct counterexamples to Statement (B). More precisely, for each prime p, we find a supersingular elliptic curve over a field $k \supset \mathbb{F}_p$ which is not trained.

We need some fine arithmetic results of definite quaternion $\mathbb{Q}$-algebras; for example see [12, Proposition 3.1, p. 145]. Let H be a definite quaternion $\mathbb{Q}$-algebra, $\mathcal{O}$ a maximal order in H and $G = \mathcal{O}^\times$. Then G is a cyclic group of order $2, 4$ or 6 except when $H = B_{2,\infty}$ or $H = B_{3,\infty}$.

When $H = B_{2,\infty} = (-1, -1/\mathbb{Q})$, the class number $h(\mathcal{O}) = 1$. Thus, any maximal order is conjugate to $\mathcal{O}$ and the mass formula gives $\#G = 24$. We also have

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

When $H = B_{3,\infty} = (-1, -3/\mathbb{Q})$, the class number $h(\mathcal{O}) = 1$. Similarly, any maximal order is conjugate to $\mathcal{O}$ and the mass formula gives $\#G = 12$. The group G is the dihedral group D_{12} of order 12 in this case.

Let E_0 be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ with Frobenius morphism $\pi_{E_0} = -p$. The endomorphism algebra $\mathrm{End}^0(E_0)$ is isomorphic to $B_{p,\infty}$, and $\mathrm{End}(E_0)$ is a maximal order in $\mathrm{End}^0(E_0) = B_{p,\infty}$. Put $G = \mathrm{Aut}(E_0)$.

Let $m > 1$ be an integer with $m \mid p^2 - 1$ and $\zeta_m \in \mathbb{F}_{p^2}^\times$ an element of order m. Set $k := \mathbb{F}_{p^2}(T)$ 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 $\sigma_m(T^{1/m}) = \zeta_m T^{1/m}$. 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 $G = \mathrm{Aut}(E_0 \otimes K)$.

The set $E(K/k, E_0 \otimes k)$ of K/k-forms of $E_0 \otimes k$ is isomorphic to

$$H^1(\mathrm{Gal}(K/k), G) \simeq \mathrm{Hom}(\mathrm{Gal}(K/k), G)/G \simeq \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, G)/G, \tag{3.1}$$

where G acts $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, G)$ by conjugation.

Take $m = 3$ if $p = 2$ and $m = 2$ if p is odd. Then the set $E(K/k, E_0 \otimes k)$ contains a non-trivial class as G contains an element of order 3 or 2 according as $p = 2$ or p is odd. Now take an elliptic curve E/k in a non-trivial class. We claim that E is not defined over $\mathbb{F}_{p^2}$. Suppose contrarily that there is an elliptic curve E_0' over $\mathbb{F}_{p^2}$ and a k-isomorphism $E_0' \otimes k \simeq E$. Since $E \otimes_k K \xrightarrow{\sim} E_0 \otimes_{\mathbb{F}_{p^2}} K$, there is a K-isomorphism $\varphi : E_0' \otimes_{\mathbb{F}_{p^2}} K \xrightarrow{\sim} E_0 \otimes_{\mathbb{F}_{p^2}} K$. Clearly $K/\mathbb{F}_{p^2}$ is primary, by Lemma 2.3 φ is defined over $\mathbb{F}_{p^2}$. This gives an isomorphism $E \simeq E_0' \otimes k \simeq E_0 \otimes_{\mathbb{F}_{p^2}} k$, a contradiction.

3.2. Endomorphism algebras $\mathrm{End}^0(E)$. Let $p = 2$ and $m = 3$. By (3.1) let $\xi \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, G)$ represent the 1-cocycle with $\xi_{\sigma_m} = \omega$, where $\omega \in G$ is an element of order 3. Let $E \in E(K/k, E_0 \otimes k)$ be a member corresponding to $\{\xi_\sigma\}$. By (2.1) we have

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

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

Let p be an odd prime and $m = 2$. Let $\xi \in \mathrm{Hom}(\mathrm{Gal}(K/k), G)$ represent the 1-cocycle with $\xi_{\sigma_2} = -1$, and E the corresponding elliptic curve over k. By (2.1) again we get $\mathrm{End}^0(E) \simeq B_{p,\infty}$.

4. Proof of Theorem 1.3

4.1. Part (1): case $p = 2, 3$. We shall 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. [8, p. 298]), that is, the Hilbert irreducibility theorem for L holds. In particular the rational function field $\mathbb{F}_q(T)$ is Hilbertian.

Let $E_0/\mathbb{F}_{p^2}$ and $k = \mathbb{F}_{p^2}(T)$ be as in Section 3. 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 [3, 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 Section 3.2, $\mathrm{End}^0(E)$ 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 D_{12}; see [3, Remark, p. 29]. Choose an isomorphism $\xi : \mathrm{Gal}(K/k) \xrightarrow{\sim} D_{12} = G$ and let $E \in E(K/k, E_0 \otimes k)$ be the member corresponding to the 1-cocycle $\{\xi_\sigma\}$. In the same way as before $\mathrm{End}^0(E)$ is isomorphic to the centralizer of D_{12} in $B_{3,\infty}$ and hence $\mathrm{End}^0(E) = \mathbb{Q}$.

4.2. Part (1): case $p > 3$. Since $p \not\equiv 1 \pmod{12}$, $p \equiv 3 \pmod 4$ 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 $y^2 = x^3 + 1$. 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 $\zeta_m \notin \mathbb{F}_p^\times$. Put $K = \mathbb{F}_{p^2}(T^{1/m})$ and $k_2 = \mathbb{F}_{p^2}(T)$. Then K/k is finite Galois with 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 have $c(\eta) = \eta^{-1}$.

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

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

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

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

Put $\sigma = \tau$, then $a \in \mathbb{Q}(\eta)$. Put $\sigma = c$, then $c(a) = a$. Thus, $\mathrm{End}^0(E) = \mathbb{Q}$.

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

Lemma 4.1. *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 not equal to $\mathbb{Q}$.*

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 4.2. *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 4.1). 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 2.3, $\mathrm{End}^0(E_0 \otimes k) = \mathrm{End}^0(E_0 \otimes \mathbb{F}_q) = \mathbb{Q}(\sqrt{-p})$. Our assumption of p implies that $\mathrm{Aut}(E_0 \otimes K) = \{\pm 1\}$ (see [2, Table 1.3, p. 117]), which is contained in the center of $\mathrm{End}(E_0 \otimes K)$. Finally by (2.1) one has

$$\begin{aligned} \mathrm{End}^0(E) &\simeq \{a \in \mathrm{End}^0(E_0 \otimes K) \mid \sigma(a) = a, \ \forall \sigma \in \mathrm{Gal}(K/k)\} \\ &= \mathrm{End}^0(E_0 \otimes k) \simeq \mathbb{Q}(\sqrt{-p}). \quad ∎ \end{aligned} \tag{4.1}$$

Acknowledgments

The author is grateful to Ching-Li Chai for helpful discussions on Propositon 2.1. The present work is done while 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 is partially supported by the grants MoST 100-2628-M-001-006-MY4 and 103-2918-I-001-009.

References

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

[2] 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.

[3] 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.
[4] K.-Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties.* Lecture Notes in Math., vol. 1680, Springer-Verlag, 1998.
[5] D. Mumford, *Abelian Varieties.* Oxford University Press, 1974.
[6] 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.
[7] F. Oort, Which abelian surfaces are products of elliptic curves? *Math. Ann.* **214** (1975), 35–47.
[8] A. Schinzel, *Polynomials with special regard to reducibility.* Encyclopedia of Mathematics and its Applications 77. Cambridge University Press, 2000. 558 pp.
[9] J. Tate, Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2** (1966), 134–144.
[10] W. C. Waterhouse, Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560.
[11] A. Weil, The field of definition of a variety. *Amer. J. Math.* **78** (1956), 509–524.
[12] M.-F. Vignéras, Arithmétique des algèbres de quaternions. Lecture Notes in Math., vol. 800, Springer-Verlag, 1980.
[13] C.-F. Yu, The isomorphism classes of abelian varieties of CM-type. *J. Pure Appl. Algebra* **187** (2004) 305–319.
[14] C.-F. Yu, Endomorphism algebras of QM abelian surfaces. *J. Pure Appl. Algebra* **217** (2013), 907–914.

Institute of Mathematics, Academia Sinica and NCTS (Taipei Office), 6th Floor, Astronomy Mathematics Building, No. 1, Roosevelt Rd. Sec. 4, Taipei, Taiwan, 10617
E-mail address: `chiafu@math.sinica.edu.tw`

The Max-Planck-Institut für Mathematik, Vivatsgasse 7, Bonn, Germany 53111
E-mail address: `chiafu@mpim-bonn.mpg.de`