Math. Res. Lett. **17** (2010), *no.* 2, 357–370

ON FINITENESS OF ENDOMORPHISM RINGS OF ABELIAN VARIETIES

Chia-Fu Yu

Abstract. The endomorphism ring End(A) of an abelian variety A is an order in a semi-simple algebra over $\mathbb{Q}$. The co-index of End(A) is the index to a maximal order containing it. We show that for abelian varieties of fixed dimension over any field of characteristic $p > 0$, the p-exponents of the co-indices of their endomorphism rings are bounded. We also give a few applications to this finiteness result.

1. Introduction

Endomorphism algebras of abelian varieties are important objects for studying abelian varieties. For example, a theorem of Grothendieck tells us that any isogeny class of abelian varieties over a field of characteristic $p > 0$ that has sufficient many complex multiplications is defined over a finite field. See Oort [12] and [22] for more details. Endomorphism algebras have been studied extensively in the literature; see Oort [13] for many detailed and interesting discussions and quite complete references therein. Thanks to Tate [20], Zarhin [24], Faltings [5], and de Jong [2], we have now a fundamental approach using Tate modules (and its analogue at p) to study these endomorphism algebras. However, not much is known for their endomorphism rings except for the one-dimensional case (see Theorem 1.4). In [21] Waterhouse determined all possible endomorphism rings for ordinary elementary abelian varieties over a finite field (see [21], Theorem 7.4 for more details).

Let A_0 be an abelian variety over a field k. Denote by $[A_0]_k$ the isogeny class of A_0 over k. It is well-known that the endomorphism ring $\mathrm{End}(A_0)$ is an order of the semi-simple $\mathbb{Q}$-algebra $\mathrm{End}^0(A_0) := \mathrm{End}(A_0) \otimes \mathbb{Q}$. A general question is what we can say about the endomorphism rings End(A) of abelian varieties A in the isogeny class $[A_0]_k$. In the paper we consider the basic question: how many isomorphism classes of the endomorphism rings End(A) of abelian varieties A in a fixed isogeny class $[A_0]_k$?

We define a natural numerical invariant for orders in a semi-simple algebra which measures how far it is from a maximal order. Let B be a finite-dimensional semi-simple algebra over $\mathbb{Q}$, and O an order of B. Define the *co-index of* O, which we denote ci(O), to be the index $[R : O]$, where R is a maximal order of B containing O. The invariant ci(O) is independent of the choice of R (see Lemma 2.1). For any prime ℓ, let v_ℓ be the discrete valuation on $\mathbb{Q}$ at the prime ℓ normalized so that $v_\ell(\ell) = 1$. The main results of this paper are:

Received by the editors May 1, 2009. Revision received February 22, 2010.

Theorem 1.1. *Let $g \geq 1$ be an integer. There is an positive integer N only depending on g such that $v_p(\mathrm{ci}(\mathrm{End}(A))) < N$ for any g-dimensional abelian variety over any field of characteristic $p > 0$.*

Theorem 1.2. *Let $g \geq 1$ be an integer. There are only finitely many isomorphism classes of rings $\mathrm{End}(A) \otimes \mathbb{Z}_p$ for all g-dimensional abelian varieties A over any field of characteristic $p > 0$.*

One can also deduce easily from Theorem 1.1 the following:

Corollary 1.3. *Let $g \geq 1$ be an integer. There are only finitely many isomorphism classes of endomorphism rings of g-dimensional supersingular abelian varieties over an algebraically closed field k of characteristic $p > 0$.*

As pointed out by the referee, Theorem 1.1 generalizes the following classical result of Deuring [4]. See Lang's book [7], Chapter 13 for a modern exposition.

Theorem 1.4 (Deuring). *Let E be an elliptic curve over an algebraically closed field of prime characteristic p. Then its endomorphism ring $\mathrm{End}(E)$ is either $\mathbb{Z}$, a maximal order in the definite quaternion $\mathbb{Q}$-algebra of discriminant p, or an order in an imaginary quadratic field whose conductor is prime to p. In particular, the index of $\mathrm{End}(E)$ in a maximal order of $\mathrm{End}^0(E)$ is prime to p.*

Note that by a theorem of Li-Oort [8], the supersingular locus $\mathcal{S}_g$ of the Siegel moduli space $\mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ has dimension $[g^2/4]$. In particular, there are infinitely many non-isomorphic supersingular abelian varieties. It is a priori not obvious why there should be only finitely many isomorphism classes in their endomorphism rings. However, since all of them are given by an isogeny of degree $p^{g(g-1)/2}$ from a superspecial one (see Li-Oort [8]), the finiteness result might be expected. This is indeed the idea of proving Theorem 1.1.

The proof of Theorem 1.1 uses the following universal bounded property due to Manin [9]: for a fixed integer $h \geq 1$, the degrees of the *minimal isogenies* $\varphi : X_0 \to X$, for all p-divisible groups X of height h over an algebraically closed field of fixed characteristic p, are bounded. See Section 4 for the definition and properties of minimal isogenies. F. Oort asks (in a private conversation) the following question: if X is equipped with an action ι by an order $\mathcal{O}$ of a finite-dimensional semi-simple algebra over $\mathbb{Q}_p$, is there an action ι_0 of $\mathcal{O}$ on X_0 so that the minimal isogeny φ becomes $\mathcal{O}$-linear? Clearly, such a map $\iota_0 : \mathcal{O} \to \mathrm{End}(X_0)$ is unique if it exists. The motivation of this question is looking for a good notion of minimal isogenies when one considers abelian varieties with additional structures (polarizations and endomorphisms). We confirm his question with positive answer in Section 4 (see Proposition 4.8). This also plays a role in the proof of Theorem 1.1.

Theorem 1.1 is sharp at least when the ground field k is algebraically closed. Namely, for any prime $\ell \neq \mathrm{char}(k)$, the finiteness for $v_\ell(\mathrm{ci}(\mathrm{End}(A)))$ does not hold in general. Indeed, we show (see Section 5)

Proposition 1.5. *Let p be a prime number or zero. There exists an abelian variety A_0 over an algebraically closed field k of characteristic p so that for any prime $\ell \neq p$ and any integer $n \geq 1$, there exists an $A \in [A_0]_k$ such that $v_\ell(\mathrm{ci}(\mathrm{End}(A))) \geq n$.*

In fact, elliptic curves already provide such examples in Proposition 1.5. For these examples, there are infinitely many isomorphism classes of rings $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ in the isogeny class for each prime ℓ prime to the characteristic of ground field.

The finiteness result (Corollary 1.3) gives rise to a new refinement on the supersingular locus $\mathcal{S}_g$ arising from arithmetic. We describe now this "arithmetic" refinement in the special case where $g = 2$. Let V be an irreducible component of the supersingular locus $\mathcal{S}_2$ in the Siegel 3-fold (with an auxiliary prime-to-p level structure) over $\overline{\mathbb{F}}_p$. It is known that V is isomorphic to $\mathbf{P}^1$ over $\overline{\mathbb{F}}_p$. We fix an isomorphism and choose an appropriate $\mathbb{F}_{p^2}$-structure on V (see Subsection 5.3 for details). For any point x in the Siegel moduli space, write $c_p(x)$ for $v_p(\mathrm{ci}(\mathrm{End}(A_x)))$, where A_x is the underlying abelian variety of the object (A_x, λ_x, η_x) corresponding to the point x. For each integer $m \geq 0$, let

$$V_m := \{x \in V; c_p(x) \leq m\}.$$

The collection $\{V_m\}_{m\geq 0}$ forms an increasing sequence of closed subsets of $V = \mathbf{P}^1$. We have (see Subsection 5.4)

$$V_0 = \cdots = V_3 \subset V_4 = V_5 \subset V_6 = V,$$

and

$$V_0 = \mathbf{P}^1(\mathbb{F}_{p^2}), \quad V_4 = \mathbf{P}^1(\mathbb{F}_{p^4}).$$

This refines the standard consideration on $\mathcal{S}_2$ by superspecial and non-superspecial points.

This paper is organized as follows. Sections 2-4 are devoted to the proof of Theorems 1.1 and 1.2. Section 2 reduces to an analogous statement for p-divisible groups over an algebraically closed field. Section 3 provides necessary information about minimal Dieudonné modules. In Section 4 we use minimal isogenies to conclude the finiteness of co-indices of endomorphism rings of p-divisible groups, and finish the proof of Theorem 1.2. Section 5 provides examples which particularly show that the ℓ-co-index of the endomorphism rings can be arbitrarily large for any prime $\ell \neq p$. A special case for the "arithmetic" refinement is treated there.

2. Reduction steps of Theorem 1.1

2.1. Co-Index. Let K be a number field, and O_K the ring of integers. Denote by K_v the completion of K at a place v of K, and O_{K_v} the ring of integers when v is finite. Let B be a finite-dimensional semi-simple algebra over K, and let O be an O_K-order of B. The *co-index* of O, written as $\mathrm{ci}(O)$, is defined to be the index $[R : O]$, where R is a maximal order of B containing O. We define the co-index similarly for an order of a finite-dimensional semi-simple algebra over a p-adic local field. For each finite place v of K, we write $R_v := R \otimes_{O_K} O_{K_v}$ and $O_v := O \otimes_{O_K} O_{K_v}$. From the integral theory of semi-simple algebras (see Reiner [16]), each R_v is a maximal order of $B \otimes_K K_v$ and we have $R/O \simeq \oplus_v R_v/O_v$, where v runs through all finite places of K. It follows that

$$\mathrm{ci}(O) = \prod_{v:\mathrm{finite}} \mathrm{ci}(O_v), \quad \mathrm{ci}(O_v) := [R_v : O_v]. \tag{2.1}$$

As the algebra B is determined by O, the co-index $\mathrm{ci}(O)$ makes sense without mentioning the algebra B containing it.

Lemma 2.1. *The co-index* $\mathrm{ci}(O)$ *is independent of the choice of a maximal order containing it.*

Proof. Using the product formula (2.1), it suffices to show the local version of the statement. Therefore, we may assume that K is a p-adic local field. If R' is another maximal order containing O, then $R' = gRg^{-1}$ for some element $g \in B^\times$. Since in this case $[R : O] = \mathrm{vol}(R)/\mathrm{vol}(O)$ for any Haar measure on B, the statement then follows from the equality $\mathrm{vol}(R) = \mathrm{vol}(gRg^{-1})$. □

2.2. Base change.

Lemma 2.2. *Let A be an abelian variety over a field k and let k' be a field extension of k, then the inclusion* $\mathrm{End}_k(A) \to \mathrm{End}_{k'}(A \otimes k')$ *is co-torsion-free, that is, the quotient is torsion free. Furthermore, we have*

$$\mathrm{ci}[\mathrm{End}_k(A)] \mid \mathrm{ci}[\mathrm{End}_{k'}(A \otimes k')]. \tag{2.2}$$

Proof. The first statement follows from Oort [13], Lemma 2.1. For the second statement, we choose a maximal order O_1 of $\mathrm{End}^0_k(A)$ containing $\mathrm{End}_k(A)$. Let O_2 be a maximal order of $\mathrm{End}^0_{k'}(A \otimes k')$ containing O_1 and $\mathrm{End}_{k'}(A \otimes k')$. Since $\mathrm{End}_k(A) = \mathrm{End}^0_k(A) \cap \mathrm{End}_{k'}(A \otimes k')$, we have the inclusion $O_1/\mathrm{End}_k(A) \subset O_2/\mathrm{End}_{k'}(A \otimes k')$. This proves the lemma. □

By Lemma 2.2, we can reduce Theorem 1.1 to the case where k is algebraically closed.

2.3. Reduction to p-divisible groups.

Lemma 2.3. *Let A be an abelian variety over a field k. Let ℓ be a prime, possibly equal to* $\mathrm{char}(k)$. *The inclusion map* $\mathrm{End}_k(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}_k(A[\ell^\infty])$ *is co-torsion-free. Here $A[\ell^\infty]$ denotes the associated ℓ-divisible group of A.*

Proof. When $\ell \neq \mathrm{char}(k)$, this is elementary and well-known; see Tate [20], p. 135. The same argument also shows the case when $\ell = \mathrm{char}(k)$. □

We remark that for an arbitrary ground field k, the endomorphism algebra $\mathrm{End}^0_k(A[\ell^\infty]) := \mathrm{End}_k(A[\ell^\infty]) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of the associated ℓ-divisible group $A[\ell^\infty]$ of an abelian variety A over k, where ℓ is a prime $\neq \mathrm{char}(k)$, may not be semi-simple; see Subsection 5.5. Therefore, the numerical invariant $\mathrm{ci}(\mathrm{End}_k(A[\ell^\infty]))$ may not be defined in general. Analogously, in the case where $\mathrm{char}(k) = p > 0$, the endomorphism algebra $\mathrm{End}^0_k(X) := \mathrm{End}_k(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of a p-divisible group X over k may not be semi-simple, and hence the numerical invariant $\mathrm{ci}(\mathrm{End}_k(X))$ may not be defined in general, either. See Subsection 5.6. However, when the ground field k is algebraically closed, both $\mathrm{ci}(\mathrm{End}(A[\ell^\infty]))$ and $\mathrm{ci}(\mathrm{End}(A[p^\infty]))$ are always defined for any abelian variety A.

Lemma 2.4. *Let A be an abelian variety over an algebraically closed field k of characteristic $p > 0$. Then one has*

$$v_p(\mathrm{ci}(\mathrm{End}_k(A))) \le v_p(\mathrm{ci}(\mathrm{End}_k(A[p^\infty]))). \tag{2.3}$$

PROOF. Let R be a maximal order of $\mathrm{End}(A) \otimes \mathbb{Q}_p$ containing $\mathrm{End}(A) \otimes \mathbb{Z}_p$. Then there is an isogeny $\varphi : A \to A'$ of p-power degree over k such that $\mathrm{End}(A') \otimes \mathbb{Z}_p = R$. We may assume that the degree of this isogeny is minimal among isogenies with this property. Then we have $\mathrm{End}(A[p^\infty]) \subset \mathrm{End}(A'[p^\infty])$. As $\mathrm{End}(A) \otimes \mathbb{Q}_p \cap \mathrm{End}(A[p^\infty]) = \mathrm{End}(A) \otimes \mathbb{Z}_p$, we have the inclusion $R/(\mathrm{End}(A) \otimes \mathbb{Z}_p) \subset \mathrm{End}(A'[p^\infty])/(\mathrm{End}(A[p^\infty]))$. This yields the inequality (2.3). □

By Lemmas 2.2 and 2.4, Theorem 1.1 follows from the following theorem.

Theorem 2.5. *Let k be an algebraically closed field of characteristic $p > 0$ and let $h \geq 1$ be a fixed integer. Then there is an integer $N > 1$, depending only on h, such that for any p-divisible group X of height h over k, one has $v_p(\mathrm{ci}(\mathrm{End}(X))) \leq N$.*

3. Minimal Dieudonné modules

3.1. Notation. In Sections 3 and 4, we let k denote an algebraically closed field of characteristic $p > 0$. Let $W := W(k)$ be the ring of Witt vectors over k, and $B(k)$ be the fraction field of $W(k)$. Let σ be the Frobenius map on W and $B(k)$, respectively. For each W-module M and each subset $S \subset M$, we denote by $\langle S \rangle_W$ the W-submodule generated by S. Similarly, $\langle S \rangle_{B(k)} \subset M \otimes \mathbb{Q}_p$ denotes the vector subspace over $B(k)$ generated by S. In this paper we use the covariant Dieudonné theory. Dieudonné modules considered here are assumed to be finite and free as W-modules. Let $\mathcal{DM}$ denote the category of Dieudonné modules over k.

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

We write a Newton polygon or a slope sequence β as a finite formal sum:

$$\sum_i r_i \lambda_i \quad \text{or} \quad \sum_i r_i (a_i, b_i),$$

where each $0 \leq \lambda_i \leq 1$ is a rational number, $r_i \in \mathbb{N}$ 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 $b_i r_i$). The Manin-Dieudonné Theorem ([9], Chap. II, "Classification Theorem", p. 35) asserts that for any Dieudonné module M over k, there are distinct coprime non-negative pairs $(a_i, b_i) \neq (0, 0)$, and positive integers r_i, for $i = 1, \ldots, s$, such that there is an isomorphism of F-isocrystals

$$M \otimes \mathbb{Q}_p \simeq \bigoplus_{i=1}^{s} (M_{(a_i,b_i)} \otimes \mathbb{Q}_p)^{\oplus r_i}. \tag{3.1}$$

Moreover, the pairs (a_i, b_i) and integers r_i are uniquely determined by M. The Newton polygon of M is defined to be $\sum_{i=1}^{s} r_i (a_i, b_i)$; the rational numbers $\lambda_i = b_i/(a_i + b_i)$ are called the slopes of M. The Newton polygon of the Dieudonné module $M_{(a,b)}$ above has single slope $\lambda = b/(a+b)$.

The F-subisocrystal N_{λ_i} of $M \otimes \mathbb{Q}_p$ that corresponds to the factor $(M_{(a_i,b_i)} \otimes \mathbb{Q}_p)^{\oplus r_i}$ in (3.1) is unique and is called the *isotypic component of $M \otimes \mathbb{Q}_p$ of slope $\lambda_i = b_i/(a_i + b_i)$*. A Dieudonné module or an F-isocrystal is called *isoclinic* if it has single slope, or equivalently $M \otimes \mathbb{Q}_p$ is an isotypic component of itself.

If M is a Dieudonné module over k, the endomorphism ring $\mathrm{End}(M) = \mathrm{End}_{\mathcal{DM}}(M)$ is the ring of endomorphisms on M in the category $\mathcal{DM}$; we write $\mathrm{End}^0(M) := \mathrm{End}(M) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ for the endomorphism algebra of M. If the Newton polygon of M is $\sum_{i=1}^s r_i(a_i, b_i)$, then the endomorphism algebra of M is isomorphic to the product of the matrix algebras $M_{r_i}(\mathrm{End}^0(M_{(a_i,b_i)}))$.

Lemma 3.1.

(1) *The endomorphism algebra* $\mathrm{End}^0(M_{(a,b)})$ *is isomorphic to*

$$B(\mathbb{F}_{p^n})[\Pi'], \quad (\Pi')^n = p^b, \quad c\Pi' = \Pi'\sigma(c), \quad \forall\, c \in B(\mathbb{F}_{p^n}). \tag{3.2}$$

Therefore, $\mathrm{End}^0(M_{(a,b)})$ *is a central division algebra over* $\mathbb{Q}_p$ *of degree* n^2 *with Brauer invariant* b/n*.*

(2) *The maximal order of the division algebra* $B(\mathbb{F}_{p^n})[\Pi']$ *is* $W(\mathbb{F}_{p^n})[\Pi]$*, where* $\Pi = (\Pi')^m p^{m'}$ *for some integers* m *and* m' *such that* $bm + nm' = 1$*, subject to the following relations*

$$\Pi^n = p, \quad \text{and} \quad c\Pi = \Pi\sigma^m(c) \quad \forall\, c \in W(\mathbb{F}_{p^n}) \tag{3.3}$$

Proof. This is certainly well-known; we provide a proof for the reader's convenience. Note that using $(\Pi')^n = p^b$ one sees that the element Π in (2) independent of the choice of the integers m and m'.

(1) The F-isocrystal $N := M_{(a,b)} \otimes \mathbb{Q}_p$ is generated by the element $e_0 := 1$. Put $e_i := F^i e_0$ for $i = 1, \dots, n-1$; the vectors $e_0, \dots, e_{n-1}$ form a $B(k)$-basis for N. Since N is generated by e_0 (as an F-isocrystal) and $(F^n - p^b)e_0 = 0$, any endomorphism $\varphi \in \mathrm{End}(N)$ is determined by the vector $\varphi(e_0)$ and this vector lies in the subspace $\langle e_0, \dots, e_{n-1}\rangle_{B(\mathbb{F}_{p^n})}$. Let Π' be the element in $\mathrm{End}(N)$ such that $\Pi'(e_0) = e_1$, and for each element $c \in B(\mathbb{F}_{p^n})$, let φ_c be the endomorphism such that $\varphi_c(e_0) = ce_0$. It is not hard to see that the endomorphism algebra $\mathrm{End}(N)$ is generated by elements Π' and φ_c for all $c \in B(\mathbb{F}_{p^n})$. One checks that $\varphi_c\Pi' = \Pi'\varphi_{\sigma(c)}$ for all $c \in B(\mathbb{F}_{p^n})$. This proves the first part of (1). One extends the valuation v_p on $\mathbb{Q}_p$ naturally to the division algebra $B(\mathbb{F}_{p^n})[\Pi']$. According to the definition (we use the normalization in [15], see p. 338), the Brauer invariant is given by $v_p(\Pi')$, which is equal to b/n. Therefore, the statement (1) is proved.

(2) It is straightforward to check the relations (3.3). Using these, any element c in the division algebra $B(\mathbb{F}_{p^n})[\Pi']$ can be written uniquely as

$$c = \Pi^r(c_0 + c_1\Pi + \cdots + c_{n-1}\Pi^{n-1}),$$

for some $r \in \mathbb{Z}$ and some elements $c_i \in W(\mathbb{F}_{p^n})$ for $i = 0, \dots, n-1$ such that c_0 is a unit in $W(\mathbb{F}_{p^n})$. The valuation $v_p(c)$ is r/n. This shows that the subring $W(\mathbb{F}_{p^n})[\Pi]$ consists of elements c with $v_p(c) \geq 0$. Since any order of $B(\mathbb{F}_{p^n})[\Pi']$ is contained in the subring of elements c with $v_p(c) \geq 0$, the order $W(\mathbb{F}_{p^n})[\Pi]$ is maximal. □

According to Lemma 3.1, a Dieudonné module M or an F-isocrystal is isoclinic if and only if its endomorphism algebra is a (finite-dimensional) central simple algebra over $\mathbb{Q}_p$. A Dieudonné module M or $M \otimes \mathbb{Q}_p$ is called *isosimple* if its endomorphism algebra is a (finite-dimensional) central division algebra over $\mathbb{Q}_p$, that is, the F-isocrystal $M \otimes \mathbb{Q}_p$ is isomorphic to $M_{(a,b)} \otimes \mathbb{Q}_p$ for some pair (a, b).

3.2. Minimal Dieudonné modules. Let (a,b) be a pair as above, and let $n := a+b$. Denote by $\mathbf{M}_{(a,b)}$ the Dieudonné module over $\mathbb{F}_p$ as follows: it is generated by elements e_i, for $i \ge 0 \in \mathbb{Z}$, 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 $i \in \mathbb{Z}_{\ge 0}$. One extends the maps F and V on $\mathbf{M}_{(a,b)} \otimes W$ by σ-linearity and σ^{-1}-linearity, respectively, so that $\mathbf{M}_{(a,b)} \otimes W$ is a Dieudonné module over k.

Let $\beta = \sum_i r_i(a_i,b_i)$ be a Newton polygon. We put $\mathbf{M}(\beta) := \sum_i \mathbf{M}_{(a_i,b_i)}^{\oplus r_i}$. Note that the Dieudonné module $\mathbf{M}(\beta)$ has Newton polygon β. Write $\beta^t := \sum_i r_i(b_i,a_i)$ for the dual of β. Denote by $\mathbf{H}(\beta)$ the p-divisible group over $\mathbb{F}_p$ corresponding to the Dieudonné module $\mathbf{M}(\beta^t)$ (This is because we use the covariant theory; the Newton polygon of a p-divisible group G is equal to the dual of that of its Dieudonné module $M(G)$).

Definition 3.2. ([3], Section 5)

(1) A Dieudonné module M over k is called *minimal* if it is isomorphic to $\mathbf{M}(\beta)\otimes W$ for some Newton polygon β. In this case β is the Newton polygon of M.

(2) A p-divisible group X over k is called *minimal* if its associated Dieudonné module is so.

Let M_λ be an isoclinic Dieudonné module of slope $\lambda = \frac{b}{a+b}$ (in reduced form). There exist integers x and y such that $xa + yb = 1$. Put $N_\lambda := M_\lambda \otimes \mathbb{Q}_p$ and let $\Pi_0 := F^y V^x$ be an operator on N_λ; it is σ^{y-x}-linear and it depends on the choice of the integers x and y. Let

$$\widetilde{N}_\lambda := \{m \in N_\lambda \mid F^n m = p^b m\} \tag{3.4}$$

be the skeleton of N_λ; it is a $B(\mathbb{F}_{p^n})$-subspace that has the same dimension as N_λ, equivalently $\widetilde{N}_\lambda$ generates N_λ over $B(k)$. Since $\Pi_0 F = F\Pi_0$, the operator Π_0 leaves the subspace $\widetilde{N}_\lambda$ invariant. The restriction of Π_0 to $\widetilde{N}_\lambda$ has the following properties:

- Π_0 (on $\widetilde{N}_\lambda$) is independent of the choice of the integers x and y, and
- $\Pi_0^n = p$, $\Pi_0^b = F$ and $\Pi_0^a = V$ on $\widetilde{N}_\lambda$.

Lemma 3.3. *Notation as above. An isoclinic Dieudonné module M_λ of slope λ is minimal if and only if (i) $F^n M_\lambda = p^b M_\lambda$, and (ii) $\Pi_0(M_\lambda) \subset M_\lambda$.*

Proof. It is clear that a minimal isoclinic Dieudonné module satisfies the conditions (i) and (ii). Conversely, suppose M_λ satisfies the conditions (i) and (ii). The condition (i) implies that M_λ is generated by the skeleton $\widetilde{M}_\lambda$ over W. Since $\Pi_0\widetilde{M}_\lambda \supset \Pi_0^n\widetilde{M}_\lambda = p\widetilde{M}_\lambda$, the quotient $\widetilde{M}_\lambda/\Pi_0(\widetilde{M}_\lambda)$ is a finite-dimensional vector space over $\mathbb{F}_{p^n}$. Choose elements $f_1,\dots,f_d$ in $\widetilde{M}_\lambda$ such that they form an $\mathbb{F}_{p^n}$-basis in $\widetilde{M}_\lambda/\Pi_0(\widetilde{M}_\lambda)$. For each $i = 1,\dots,d$, the W-submodule $\langle f_i, \Pi_0(f_i), \dots, \Pi_0^{n-1}(f_i)\rangle$ is a Dieudonné submodule of M. Since F sends $\Pi_0^j(f_i)$ to $\Pi_0^{j+b}(f_i)$ and V sends $\Pi_0^j(f_i)$ to $\Pi_0^{j+a}(f_i)$, this Dieudonné module is isomorphic to $W \otimes \mathbf{M}_{(a,b)}$ by sending $\Pi_0^j(f_i)$ to e_j. Therefore, $M_\lambda \simeq W \otimes \mathbf{M}_{(a,b)}^{\oplus d}$. This proves the lemma. □

Let M be a Dieudonné module. Put $N := M \otimes \mathbb{Q}_p$. Let

$$N = \bigoplus_\lambda N_\lambda$$

be the decomposition into isotypic components. Put $M_\lambda := M \cap N_\lambda$.

Lemma 3.4.

(1) A Dieudonné module M is minimal if and only if its endomorphism ring $\mathrm{End}(M)$ *is a maximal order of* $\mathrm{End}^0(M)$.

(2) A Dieudonné module M is minimal if and only if it is isomorphic to the direct sum of its isotypic components M_λ and each factor M_λ is minimal.

Proof. (1) To prove the only if part, it suffices to show when $M = \mathbf{M}_{(a,b)}$ (for simplicity we write $\mathbf{M}_{(a,b)}$ for $\mathbf{M}_{(a,b)} \otimes W$ here). Let $n := a + b$ and $m \in \mathbb{Z}$ such that $mb \equiv 1 \mod n$. For each element $c \in W(\mathbb{F}_{p^n})$, we define an endomorphism $\varphi_c \in \mathrm{End}_{\mathcal{DM}}(\mathbf{M}_{(a,b)})$ by $\varphi_c(e_i) = \sigma^{mi}(c)e_i$ for all $i \ge 0$. Let $\Pi \in \mathrm{End}_{\mathcal{DM}}(\mathbf{M}_{(a,b)})$ be the endomorphism which sends e_i to e_{i+1}. The endomorphism ring $\mathrm{End}_{\mathcal{DM}}(\mathbf{M}_{(a,b)})$ is generated by elements Π and φ_c for all $c \in W(\mathbb{F}_{p^n})$, subject to the relations $\Pi^n = p$ and $\Pi\varphi_c = \varphi_{\sigma^{-m}(c)}\Pi$. Hence, $\mathrm{End}_{\mathcal{DM}}(\mathbf{M}_{(a,b)}) \simeq W(\mathbb{F}_{p^n})[\Pi]$ with relations $\Pi^n = p$ and $\Pi c \Pi^{-1} = \sigma^{-m}(c)$ for $c \in W(\mathbb{F}_{p^n})$. This is the maximal order in the endomorphism algebra $\mathrm{End}^0_{\mathcal{DM}}(\mathbf{M}_{(a,b)})$; see Lemma 3.1.

We prove the if part. First of all, a maximal order is isomorphic to a product of matrix rings $M_d(O_D)$, where D is a division central algebra over $\mathbb{Q}_p$ and O_D is its maximal order. Using the Morita equivalence, we can assume that $\mathrm{End}^0_{\mathcal{DM}}(M)$ is a division algebra D and $\mathrm{End}_{\mathcal{DM}}(M) = O_D$. Let $[D : \mathbb{Q}_p] = n^2$. One chooses a presentation for $O_D = W(\mathbb{F}_{p^n})[\Pi]$ with relations $\Pi^n = p$ and $\Pi c \Pi^{-1} = \sigma^{-m}(c)$ for $a \in W(\mathbb{F}_{p^n})$, for some $m \in \mathbb{Z}$. Let b be the integer such that $bm \equiv 1 \mod n$ and $0 \le b < n$. Using Lemma 3.1, the division algebra D has invariant b/n, and hence the Dieudonné module M has single slope b/n. Put $\widetilde{M} := \{x \in M; F^n x = p^b x\}$ and $\widetilde{N} := \widetilde{M \otimes \mathbb{Q}_p}$ be the skeleton of $M \otimes \mathbb{Q}_p$. It follows from $F\Pi = \Pi F$ that Π is an automorphism on $\widetilde{N}$. It follows from $\widetilde{N} \cap M = \widetilde{M}$ that for $x \in M$, one has $x \in \widetilde{M}$ if and only if $\Pi x \in \widetilde{M}$; this implies $\widetilde{M} \not\subset \Pi M$. Choose an element $e_0 \in \widetilde{M} \smallsetminus \Pi M$. Then elements $e_0, \Pi(e_0), \dots, \Pi^{n-1}(e_0)$ generate M over W. Using $F\Pi = \Pi F$ and $F^n = p^b$ on $\widetilde{M}$, one can show that $F(e_0) = \alpha \Pi^b(e_0)$ for some $\alpha \in W(\mathbb{F}_{p^n})^\times$ with $N_{W(\mathbb{F}_{p^n})/\mathbb{Z}_p}(\alpha) = 1$. By Hilbert's 90, one may replace e_0 by λe_0 so that $F(e_0) = \Pi^b(e_0)$. This shows $M \simeq \mathbf{M}_{(a,b)}$.

(2) This is clear. □

4. Construction of minimal isogenies

4.1. Minimal isogenies.

Definition 4.1. (cf. [8], Section 1) Let X be a p-divisible group over k. The minimal isogeny of X is a pair (X_0, φ) where X_0 is a minimal p-divisible group over k, and $\varphi : X_0 \to X$ is an isogeny over k 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 4.2. *Let M be a Dieudonné module over k. Then there exists a unique biggest minimal Dieudonné submodule $M_{\min}$ contained in M. Dually there is a unique smallest minimal Dieudonné module $M^{\min}$ containing M.*

PROOF. Suppose that M_1 is a minimal Dieudonné module contained in M. Then $M_{1,\lambda} \subset M_\lambda$ (see Section 3). Therefore we may assume that M is isoclinic of slope λ. If M_1 and M_2 are two minimal Dieudonné modules contained M, then M_1+M_2 satisfies the conditions (i) and (ii) in Lemma 3.3, and hence it is minimal. This completes the proof. □

The minimal Dieudonné module $M_{\min}$ is called the *minimal Dieudonné submodule* of M; the module $M^{\min}$ is called the *minimal Dieudonné overmodule* of M. By Lemma 4.2, we have

Corollary 4.3. *For any p-divisible group X over k, the minimal isogeny exists.*

Remark 4.4. For the reader who might question about ground fields, we mention that the notion of minimal isogenies can be generalized over any field of characteristic p as follows. Let X be a p-divisible group over a field K of characteristic $p>0$. We call a K-isogeny $\varphi : X_0 \to X$ *minimal* if

(i) (stronger form) X_0 is isomorphic to $\mathbf{H}(\beta) \otimes_{\mathbb{F}_p} K$, for some Newton polygon β, and φ satisfies the universal property as in Definition 4.1, or
(ii) (weaker form) the base change over its algebraic closure $\varphi_{\bar{K}} : X_{0,\bar{K}} \to X_{\bar{K}}$ is the minimal isogeny of $X_{\bar{K}}$.

Suppose that X is an etale p-divisible group over K. Then $X_{\bar{K}}$ is a minimal p-divisible group, and the identity map $id : X \to X$ is a minimal isogeny in the sense of the weaker form. However, if X is not isomorphic to the constant etale p-divisible group, then X is not isogenous over K to the constant etale p-divisible group. Therefore, X does not admit a minimal isogeny in the sense of the stronger form.

We need the following finiteness result due to Manin. This follows immediately from [9], Theorems III.3.4 and III.3.5.

Theorem 4.5. *Let $h \ge 1$ be a positive integer. Then there is an integer N only depending on h such that for all p-divisible groups X of height h over k, the degree of the minimal isogeny φ of X is less than p^N.*

Remark 4.6. Let E be the (unique up to isomorphism) supersingular p-divisible group of height two over k, and let $X_0 := E^g$. Let X be a supersingular p-divisible group of height $2g$ over k. Nicole and Vasiu showed that the kernel of the minimal isogeny $\varphi : X_0 \to X$ is annihilated by $p^{\lceil (g-1)/2 \rceil}$; see [11], Remark 2.6 and Corollary 3.2. Moreover, this is optimal, that is, there is a supersingular p-divisible group X of height $2g$ such that $\ker \varphi$ is not annihilated by $p^{\lceil (g-1)/2 \rceil -1}$; see [11], Example 3.3.

4.2. Construction of minimal isogenies. Let M be a Dieudonné module over k. Put $N := M \otimes \mathbb{Q}_p$ and let

$$N = \bigoplus_{\lambda} N_\lambda$$

be the isotypic decomposition. Let $\widetilde{N}_\lambda$ be the skeleton of N_λ (see (3.4)) and put $\widetilde{M}_\lambda := M_\lambda \cap \widetilde{N}_\lambda$. Let (a,b) be the pair associated to λ and put $n=a+b$. Write

W_0 for the ring $W(\mathbb{F}_{p^n})$ of Witt vectors over $\mathbb{F}_{p^n}$. Let $\widetilde{Q}_\lambda := W_0[\Pi_0]\widetilde{M}^t_\lambda$, the $W_0[\Pi_0]$-submodule of $\widetilde{N}^t_\lambda$ generated by $\widetilde{M}^t_\lambda$. Let $\widetilde{P}_\lambda := \widetilde{Q}^t_\lambda$ and let

$$P(M) := \bigoplus_\lambda \langle \widetilde{P}_\lambda \rangle_W. \tag{4.1}$$

We claim that

Lemma 4.7. *The Dieudonné module $P(M)$ constructed as above is the minimal Dieudonné submodule $M_{\min}$ of M.*

Proof. It is clear that $M_{\min} = \oplus M_{\min,\lambda}$ and $M_{\min,\lambda}$ is the minimal Dieudonné submodule of M_λ. Therefore, it suffices to check $\widetilde{P}_\lambda = \widetilde{M}_{\min,\lambda}$. As $\widetilde{M}_{\min,\lambda} \subset \widetilde{M}_\lambda$, $\widetilde{M}_{\min,\lambda}$ is the minimal Dieudonné submodule of $\widetilde{M}_\lambda$. Taking dual, it suffices to show that $\widetilde{Q}_\lambda$ is the minimal Dieudonné overmodule of $\widetilde{M}^t_\lambda$. This then follows from Lemma 3.3. □

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 4.8. *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. Let M be the Dieudonné module of X and let $\phi \in \mathrm{End}_{\mathcal{DM}}(M)$ be an endomorphism. It suffices to show that $\phi(M_{\min}) \subset M_{\min}$. It is clear that $\phi(\widetilde{N}_\lambda) \subset \widetilde{N}_\lambda$. It follows from the construction of the minimal Dieudonné submodule that $\phi(M_{\min}) \subset M_{\min}$. This proves the proposition. □

4.3. Proof of Theorem 2.5. Let M be the Dieudonné module of X. Let $M^{\min}$ be the minimal Dieudonné overmodule of M. By Theorem 4.5, there is a positive integer N_1 only depending on the rank of M such that the length length$(M^{\min}/M)$ as a W-module is less than N_1. Let N_2 be a positive integer so that $p^{N_2}M^{\min} \subset M \subset M^{\min}$. Let $\phi \in \mathrm{End}_{\mathcal{DM}}(M)$ be an element. By Proposition 4.8, one has $\phi \in \mathrm{End}_{\mathcal{DM}}(M^{\min})$. Therefore, we have showed

$$\mathrm{End}_{\mathcal{DM}}(M) = \{\phi \in \mathrm{End}_{\mathcal{DM}}(M^{\min})\,;\, \phi(M) \subset M\}. \tag{4.2}$$

We claim that $p^{N_2}\,\mathrm{End}_{\mathcal{DM}}(M^{\min}) \subset \mathrm{End}_{\mathcal{DM}}(M)$. Indeed, if $\phi \in \mathrm{End}_{\mathcal{DM}}(M^{\min})$, then

$$p^{N_2}\phi(M) \subset p^{N_2}M^{\min} \subset M.$$

Therefore, there is an positive integer N only depending on the rank of M such that $v_p(\mathrm{ci}(\mathrm{End}_{\mathcal{DM}}(M))) < N$. This completes the proof of Theorem 2.5, and hence completes the proof of Theorem 1.1.

4.4. Proof of Theorem 1.2. By a theorem of Tate [20], we have

$$[\mathrm{End}^0(A)\otimes\mathbb{Q}_p:\mathbb{Q}_p]\le 4g^2.$$

Since there are finitely many finite extensions of $\mathbb{Q}_p$ of bounded degree, and finitely many Brauer invariants with bounded denominator, there are finitely many semi-simple algebras $\mathrm{End}^0(A)\otimes\mathbb{Q}_p$, up to isomorphism, of abelian varieties A of dimension g. It follows from Theorem 1.1 that in each isogeny class there are finitely many endomorphism rings $\mathrm{End}(A)\otimes\mathbb{Z}_p$, up to isomorphism. Therefore, there are finitely many isomorphism classes of the endomorphism rings $\mathrm{End}(A)\otimes\mathbb{Z}_p$ for all g-dimensional abelian varieties A of a field of characteristic $p>0$. This completes the proof.

5. Examples

5.1. We start with a trivial example. Suppose the abelian variety A_0 over a field k has the property $\mathrm{End}_k(A_0)=\mathbb{Z}$. Then for any member $A\in[A_0]_k$, the endomorphism ring $\mathrm{End}_k(A)$ is always a maximal order. Therefore, there is an isogeny class $[A_0]_k$ such that the endomorphism rings $\mathrm{End}_k(A)$ are maximal for all $A\in[A_0]_k$.

5.2. Let p be any prime number. Let K be an imaginary quadratic field such that p splits in K. Let O_K be the ring of integers. For any positive integer m, let $E^{(m)}$ be the elliptic curve over $\mathbb{C}$ so that $E^{(m)}(\mathbb{C})=\mathbb{C}/\mathbb{Z}+mO_K$. It is easy to see that $\mathrm{End}_{\mathbb{C}}(E^{(m)})=\mathbb{Z}+mO_K$, and hence $\mathrm{ci}(\mathrm{End}(E^{(m)}))=m$. By the theory of complex multiplication [19], each elliptic curve $E^{(m)}$ is defined over $\bar{\mathbb{Q}}$ and has good reduction everywhere over some number field. Let $E_p^{(m)}$ be the reduction of $E^{(m)}$ over $\overline{\mathbb{F}}_p$; this is well-defined. Since $O_K\otimes\mathbb{Z}_p$ has non-trivial idempotent and hence it is not contained in the division quaternion $\mathbb{Q}_p$-algebra, $E_p^{(m)}$ is ordinary. Therefore, we have $\mathrm{End}(E_p^{(m)})\otimes\mathbb{Z}_p=\mathbb{Z}_p\times\mathbb{Z}_p$ is maximal (see [4], cf. [7], Chapter 13, Theorem 5, p. 175). Clearly we have $E^{(m)}\in[E^{(1)}]_{\overline{\mathbb{Q}}}$ and $E_p^{(m)}\in[E_p^{(1)}]_{\overline{\mathbb{F}}_p}$. Using [13], Lemma 2.1, we show that for $(m,p)=1$, $\mathrm{ci}(\mathrm{End}(E_p^{(m)}))=\mathrm{ci}(\mathrm{End}(E^{(m)})=m$. These give examples over a field characteristic zero or $p>0$ in Proposition 1.5.

Note that not all of elliptic curves $E^{(m)}$ (resp. $E_p^{(m)}$) above are defined over a fixed number field (resp. a fixed finite field). Therefore, we did not exhibit an example for Proposition 1.5 when the ground k is of finite type over its prime subfield. In the case where k is a finite field or a number field, there are only finitely many isomorphism classes over k in an isogeny class $[A_0]_k$ (see Milne [10], Chap. I, Corollary 13.13, p. 61 and Chap. VI, Theorem 1.1, p. 131). In particular, the co-index $\mathrm{ci}(\mathrm{End}(A))$ is bounded for $A\in[A_0]_k$. One might expect that the latter is true when k is finitely generated over its prime subfield.

5.3. Description of $\mathcal{S}_2$. Let $n\ge 3$ be a prime-to-p positive integer. Let $\mathcal{A}_{2,1,n}\otimes\overline{\mathbb{F}}_p$ denote the Siegel 3-fold over $\overline{\mathbb{F}}_p$ with level n-structure, and let $\mathcal{S}_2$ denote the supersingular locus. Let Λ^* be the set of isomorphism classes of superspecial polarized abelian surfaces (A,λ,η) over $\overline{\mathbb{F}}_p$ with polarization degree $\deg\lambda=p^2$ and a level n-structure η. For each member $\xi=(A_1,\lambda_1,\eta_1)\in\Lambda^*$, let S_ξ be the space that parametrizes degree p isogenies $\varphi:(A_1,\lambda_1,\eta_1)\to(A,\lambda,\eta)$ preserving polarizations and level structures. The variety S_ξ is isomorphic to $\mathbf{P}^1$ over $\overline{\mathbb{F}}_p$; we impose the $\mathbb{F}_{p^2}$-structure on $\mathbf{P}^1$ defined by $F^2=-p$ on M_1, where M_1 is the Dieudonné module of A_1 and F is the Frobenius map on M_1. For this structure, the superspecial points are exactly the $\mathbb{F}_{p^2}$-valued points on V. It is known (see Katsura-Oort [6]) that the projection $\mathrm{pr} : S_\xi \to \mathcal{S}_2$ induces an isomorphism $\mathrm{pr} : S_\xi \simeq V_\xi \subset \mathcal{S}_2$ onto one irreducible component. Conversely, any irreducible component V is of the form V_ξ for exact one member $\xi \in \Lambda^*$. Two irreducible components V_1 and V_2, if they intersect, intersect transversally at some superspecial points.

5.4. "Arithmetic" refinement of $\mathcal{S}_2$. We describe the arithmetic refinement on one irreducible component $V = \mathbf{P}^1$ of $\mathcal{S}_2$. For any point x, we write $c_p(x)$ for $v_p(\mathrm{ci}(\mathrm{End}(A_x)))$, where A_x is the underlying abelian surface of the object (A_x, λ_x, η_x) corresponding to the point x. Let D be the division quaternion algebra over $\mathbb{Q}_p$ and let O_D be the maximal order of D. The endomorphism ring of a superspecial Dieudonné module is (isomorphic to) $M_2(O_D)$. For non-superspecial supersingular Dieudonné modules, one can compute their endomorphism rings using (4.2). Let $\pi : M_2(O_D) \to M_2(\mathbb{F}_{p^2})$ be the natural projection. We compute these endomorphism rings and get (see [23], Proposition 3.2):

Proposition 5.1. *Let x be a point in $V = \mathbf{P}^1$ and let M_x be the associated Dieudonné module.*

(1) *If $x \in \mathbf{P}^1(\mathbb{F}_{p^2})$, then* $\mathrm{End}_{\mathcal{DM}}(M_x) = M_2(O_D)$.

(2) *If $x \in \mathbf{P}^1(\mathbb{F}_{p^4}) - \mathbf{P}^1(\mathbb{F}_{p^2})$, then*

$$\mathrm{End}_{\mathcal{DM}}(M_x) \simeq \{\phi \in M_2(O_D)\,;\pi(\phi) \in B_0'\,\},$$

where $B_0' \subset M_2(\mathbb{F}_{p^2})$ is a subalgebra isomorphic to $\mathbb{F}_{p^2}(x)$.

(3) *If $x \in \mathbf{P}^1(k) - \mathbf{P}^1(\mathbb{F}_{p^4})$, then*

$$\mathrm{End}_{\mathcal{DM}}(M_x) \simeq \left\{ \phi \in M_2(O_D)\,;\pi(\phi) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},\, a \in \mathbb{F}_{p^2} \right\}.$$

We remark that Proposition 5.1 was also known to Ibukiyama.

For each integer $m \geq 0$, let

$$V_m := \{x \in V; c_p(x) \leq m\}.$$

The collection $\{V_m\}_{m\geq 0}$ forms an increasing sequence of closed subsets of $V = \mathbf{P}^1$. We apply Proposition 5.1 and get

$$V_0 = \cdots = V_3 \subset V_4 = V_5 \subset V_6 = V,$$

and

$$V_0 = \mathbf{P}^1(\mathbb{F}_{p^2}), \quad V_4 = \mathbf{P}^1(\mathbb{F}_{p^4}).$$

This provides more information on $\mathcal{S}_2$ not just superspecial and non-superspecial points.

5.5. Semi-simplicity of Tate modules. Let A be an abelian variety over a field k. Let k^{sep} a separable closure of k and let $G := \mathrm{Gal}(k^{sep}/k)$ be the Galois group. To each prime $\ell \neq \mathrm{char}(k)$, one associates the ℓ-adic Galois representation

$$\rho_\ell : G \to \mathrm{Aut}(T_\ell(A)),$$

where $T_\ell(A)$ is the Tate module of A. According to Faltings [5] and Zarhin [24], under the condition that the ground field k is of finite type over its prime field, the

Tate module $V_\ell := T_\ell(A) \otimes \mathbb{Q}_\ell$ is semi-simple as a $\mathbb{Q}_\ell[G]$-module. We show that this condition is necessary.

Let A_0 be an abelian variety over a field k_0 which is finitely generated over its prime field. We write $G_0 := \mathrm{Gal}(k_0^{\mathrm{sep}}/k_0)$ and G_0^{alg} for the algebraic envelope of $G_\ell := \rho_\ell(G_0)$; that is, G_0^{alg} is the Zariski closure of G_ℓ in $\mathrm{Aut}(V_\ell(A_0))$ that is regarded as algebraic groups over $\mathbb{Q}_\ell$. Assume that the algebraic group G_0^{alg} is not a torus; for example let A_0 be an elliptic curve without CM. We shall choose an intermediate subfield $k_0 \subset k \subset k_0^{\mathrm{sep}}$ so that the Tate module $V_\ell(A)$ associated to the base change $A := A_0 \otimes k$ is not semi-simple as a $G := \mathrm{Gal}(k^{\mathrm{sep}}/k)$-module. We can choose a closed subgroup $H \subset G_\ell$ such that $V_\ell(A_0)$ is not a semi-simple $\mathbb{Q}_\ell[H]$-module. To see this, by Bogomolov's theorem (see [1]), G_ℓ is an open compact subgroup of $G_0^{\mathrm{alg}}(\mathbb{Q}_\ell)$. We choose a Borel subgroup of B of G_0^{alg} and let H be the the intersection $G_\ell \cap B(\mathbb{Q}_\ell)$. Then H is a closed non-commutative solvable group and $V_\ell(A_0)$ is not a semi-simple $\mathbb{Q}_\ell[H]$-module. Using the Galois theory, let k correspond the closed subgroup $\rho_\ell^{-1}(H)$. Then the abelian variety $A := A_0 \otimes k$ gives a desired example.

In this example, the endomorphism algebra $\mathrm{End}_k^0(A[\ell^\infty]) = \mathrm{End}_{\mathbb{Q}_\ell[H]}(V_\ell(A))$ is not semi-simple.

5.6. Semi-simplicity of endomorphism algebras of p-divisible groups. Let k be a field of characteristic $p > 0$. Consider the following two questions:

(1) Is the category of p-divisible groups of finite height up to isogeny over k semi-simple?

(2) Is the endomorphism algebra $\mathrm{End}_k(X) \otimes \mathbb{Q}_p$ of a p-divisible group X over k semi-simple?

We show that the answers to both questions are negative. Indeed etale p-divisible groups already provide such examples. Note that the category of etale p-divisible groups of finite height up to isogeny is equivalent to the category of continuous linear representations of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on finite-dimensional $\mathbb{Q}_p$-vector spaces. For instance, one can have a 2-dimensional Galois representation whose image is the set of all upper-triangular unipotent matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$. It gives a counter-example for both questions.

Acknowledgements

Obviously the present work relies on the work of Manin [9] and uses the notion of minimal isogenies whose significance is pointed out in Li-Oort [8]. The author wishes to thank them for the influential papers. He thanks C.-L. Chai, U. Görtz, F. Oort and J.-D. Yu for helpful discussions and comments, and the referee for careful reading and helpful comments that improve the exposition significantly. The manuscript is prepared during the author's stay at Universität Bonn, and some revision is made at l'Institut des Hautes Études Scientifiques. He acknowledges the institutions for kind hospitality and excellent working conditions. The research was partially supported by grants NSC 97-2115-M-001-015-MY3 and AS-98-CDA-M01.

References

[1] F.A. Bogomolov, *Sur l'algébricité des représentations l-adiques*, C. R. Acad. Sci. Paris Sér. I Math. **290** (1980), no. 15, A701–A703.

[2] A.J. de Jong, *Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic*, Invent. Math. **134** (1998), 301–333.

[3] A.J. de Jong and F. Oort, *Purity of the stratification by Newton polygons*, J. Amer. Math. Soc. **13** (2000), 209–241.

[4] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg **14** (1941), 197–272.

[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[6] T. Katsura and F. Oort, *Families of supersingular abelian surfaces*, Compositio Math. **62** (1987), 107–167.

[7] S. Lang, *Elliptic functions.* Second edition. Graduate Texts in Mathematics, **112**. Springer-Verlag, New York, 1987.

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

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

[10] J. Milne, *Abelian varieties.* Available in http://www.jmilne.org.

[11] M.-H. Nicole and A. Vasiu, *Minimal truncations of supersingular p-divisible groups*, Indiana Univ. Math. J. **56** (2007), 2887–2897.

[12] 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.

[13] F. Oort, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, in honor of M. Nagata (1988), 469–502.

[14] F. Oort, *Minimal p-divisible groups*, Ann. Math. **161** (2005), 1021–1036.

[15] R. S. Pierce, *Associative algebras.* Graduate Texts in Mathematics, **88**. Springer-Verlag, New York-Berlin, 1982. 436 pp.

[16] I. Reiner, *Maximal orders.* London Mathematical Society Monographs, No. **5**. Academic Press, London-New York, 1975. 395 pp.

[17] V. Rotger, *Which quaternion algebras act on a modular abelian variety?* Math. Res. Lett. **15** (2008), no. 2, 251–263.

[18] J.-P. Serre, *Résumé des cours de 1984-1985*, pp. 27–32, Œuvres Collected papers. IV. 1985–1998, 2000.

[19] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions.* Publ. Math. Soc. Japan 11 (Iwanami Shoten, Tokyo, and Princeton Univ. Press, 1971).

[20] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[21] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **1969**, 521–560.

[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 and J.-D. Yu, *Mass formula for supersingular abelian surfaces*, J. Algebra **322** (2009), 3733–3743.

[24] J.G. Zarhin, *Endomorphisms of Abelian varieties over fields of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **39** (1975), 272–277 = Math. USSR-Izv. **9** (1975), 255–260.

Institute of Mathematics, Academia Sinica and NCTS (Taipei Office), 6th Floor, Astronomy Mathematics Building, No. 1, Roosevelt Rd. Sec. 4, Taipei, Taiwan

E-mail address: chiafu@math.sinica.edu.tw