# Group structures of elementary supersingular abelian varieties over finite fields

Hui Zhu
*MSRI, 1000 Centennial Drive, Berkeley, CA 94720, USA*
zhu@msri.org

Version Nov 29, 1998

**Abstract**

Let $A$ be a supersingular abelian variety over a finite field $\mathbf{k}$ which is isogenous to a power of a simple abelian variety over $\mathbf{k}$. Write the characteristic polynomial of the Frobenius endomorphism of $A$ relative to $\mathbf{k}$ as $f = g^e$ for a monic irreducible polynomial $g$ and a positive integer $e$, we show that the group of $\mathbf{k}$-rational points $A(\mathbf{k})$ on $A$ is isomorphic to $(\mathbf{Z}/g(1)\mathbf{Z})^e$ unless $A$'s simple component is of dimension 1 or 2, in which case we prove that $A(\mathbf{k})$ is isomorphic to $(\mathbf{Z}/g(1)\mathbf{Z})^a \times (\mathbf{Z}/\frac{g(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})^b$ for some non-negative integers $a, b$ with $a + b = e$. In particular, if the characteristic of $\mathbf{k}$ is 2 or $A$ is simple of dimension greater than 2, then $A(\mathbf{k}) \cong (\mathbf{Z}/g(1)\mathbf{Z})^e$.

AMS classification: 14K22, 06B15.

## 1 Introduction

We list some notation and terminology for this paper as follows: $\mathbf{k}$ is a finite field of characteristic $p$ with $q$ elements. Let $\bar{\mathbf{k}}$ be an algebraic closure of $\mathbf{k}$. Let $A$ be an abelian variety of dimension $d$ defined over $\mathbf{k}$. Let $\pi$ be the Frobenius endomorphism of $A$ relative to $\mathbf{k}$ and $f$ its characteristic polynomial.

An abelian variety over $\mathbf{k}$ is *elementary* if it is $\mathbf{k}$-isogenous to a power of a simple abelian variety over $\mathbf{k}$. This definition is different from that of [15] (see [16, page 54]). An abelian variety $A$ is elementary if and only if $f = g^e$ for some monic irreducible polynomial $g$ over $\mathbf{Q}$ and some positive integer $e$. An arbitrary abelian variety is $\mathbf{k}$-isogenous to a product of elementary abelian varieties, and $f = \prod_{i=1}^{t} g_i^{e_i}$ for distinct monic irreducible polynomials $g_i$ over $\mathbf{Q}$ and positive integers $e_i$. An abelian variety $A$ over $\mathbf{k}$ is *supersingular* if each complex root of $f$ can be written in the form $\zeta\sqrt{q}$, the product of some root of unity $\zeta$ and the positive square root $\sqrt{q}$.

**Theorem 1.1.** *Let $A$ be an elementary supersingular abelian variety over $\mathbf{k}$ and $f = g^e$ as above. Then $A(\mathbf{k})$ is isomorphic as an abelian group to $(\mathbf{Z}/g(1)\mathbf{Z})^e$ except in the following cases:*

*(1)* $p \equiv 3 \bmod 4$, *$q$ is not a square, and $A$ is* $\mathbf{k}$*-isogenous to a power of a supersingular elliptic curve with* $g = X^2 + q$,

*(2)* $p \equiv 1 \bmod 4$, *$q$ is not a square, and $A$ is* $\mathbf{k}$*-isogenous to a power of a two dimensional abelian variety with* $g = X^2 - q$.

*In these two exceptional cases, there are non-negative integers $a, b$ with $a+b=e$ such that*

$$A(\mathbf{k}) \cong (\mathbf{Z}/g(1)\mathbf{Z})^a \times \left(\mathbf{Z}/\tfrac{g(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}\right)^b.$$

This result is particularly striking when $p = 2$ or $A$ is simple with $d > 2$ for then $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^e$. In the latter case $A(\mathbf{k})$ will be either cyclic or a product of two cyclic groups, since $e = 1$ or $2$. (See Proposition 3.3).

We call an elementary supersingular abelian variety $A$ *exceptional* if it belongs to either of the two isogeny classes stated in Theorem 1.1 (1) and (2). We will show (see Proposition 3.9) that if $A$ is exceptional, then for every pair of non-negative integers $a', b'$ with $a' + b' = e$, there exists an abelian variety $A'$ which is $\mathbf{k}$-isogenous to $A$ and

$$A'(\mathbf{k}) \cong (\mathbf{Z}/g(1)\mathbf{Z})^{a'} \times \left(\mathbf{Z}/\tfrac{g(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}\right)^{b'}.$$

In this paper $\mathrm{End}_{\mathbf{k}}(A)$ denotes the ring of $\mathbf{k}$-endomorphisms of $A$. Write $\mathrm{End}^0_{\mathbf{k}}(A) = \mathrm{End}_{\mathbf{k}}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$. Let $\mathbf{Q}[\pi]$ be the $\mathbf{Q}$-subalgebra of $\mathrm{End}^0_{\mathbf{k}}(A)$ generated by $\pi$, let $\mathcal{O}$ be its maximal order, and $\mathbf{Z}[\pi]$ its $\mathbf{Z}$-subalgebra generated by $\pi$. The group $A(\bar{\mathbf{k}})$ is naturally an $\mathrm{End}_{\mathbf{k}}(A)$-module. Our results describe $A(\bar{\mathbf{k}})$ as a module over any subring of $\mathrm{End}_{\mathbf{k}}(A) \cap \mathbf{Q}[\pi]$ that contains $\pi$. For any prime number $l$ we write $R_{(l)}$ for the localization of a commutative ring $R$ at $l$, this notation should not be confused with that for the $l$-adic completion $R_l$.

**Theorem 1.2.** *Let $A$ be an elementary supersingular abelian variety over* $\mathbf{k}$ *of dimension $d$. Let $R$ be a ring with* $\mathbf{Z}[\pi] \subseteq R \subseteq \mathrm{End}_{\mathbf{k}}(A) \cap \mathbf{Q}[\pi]$. *Then there is a surjective $R$-module homomorphism*

$$\varphi : A(\bar{\mathbf{k}}) \to (R_{(p)}/R)^e$$

*such that the cardinality of the kernel of $\varphi$ divides $2^d$. Furthermore, $\varphi$ is an isomorphism when $p = 2$.*

Suppose $A$ is a simple supersingular abelian variety over $\mathbf{k}$ and $R$ the endomorphism ring $\mathrm{End}_{\mathbf{k}}(A) \cap \mathbf{Q}[\pi]$: if $d \neq 2$, then $A(\bar{\mathbf{k}}) \cong_R (R_{(p)}/R)^e$; if $d = 2$, then $A(\bar{\mathbf{k}}) \cong_R (R_{(p)}/R)^a \times (\mathcal{O}_{(p)}/\mathcal{O})^b$ for some non-negative integers $a, b$ with $a + b = e$. (See Proposition 3.8.)

The group structure of the $\mathbf{k}$-rational points and $\bar{\mathbf{k}}$-rational points on an elliptic curve were studied by [3] (see also [13, Chapter V] and [6]). The group structure of the $\mathbf{k}$-rational points on a supersingular elliptic curve can be found in [12, Chapter 4]. Descriptions of that nature for higher dimensional abelian varieties remain open. (Recently, independent of our work, the group structure of dimensional two supersingular abelian varieties was studied in [17].)

We develop the following idea for studying a supersingular abelian variety $A$ over $\mathbf{k}$: we show that the ring $\mathbf{Z}[\zeta\sqrt{q}]$ is locally almost a discrete valuation ring at every prime; in fact it is a *Bass order* over some suitable subring (see section 2). Next we describe the Tate modules of $A$ over $\mathbf{Z}[\pi]$. Finally the group structure of $A(\mathbf{k})$ follows by viewing $A(\mathbf{k})$ as the kernel of the isogeny $\pi - 1$ on $A(\bar{\mathbf{k}})$ (see section 3). The group and module structures on an arbitrary supersingular abelian varieties over finite fields are studied in [18].

This paper is based on a portion of the author's Berkeley Ph.D thesis. The author is deeply grateful to her advisor Professor Hendrik Lenstra for inspiration and guidance. The author also wish to thank Bjorn Poonen and Phil Ryan for their comments on an earlier version of this paper. The author was supported as a MSRI postdoctoral fellow while preparing this paper.

# 2 Torsion-free modules over Bass orders

## 2.1 Orders

We begin this section by introducing some notions from commutative algebra, then we prove several auxiliary results from algebraic number theory. The material largely follows [2, Introduction and Chapter 3]. Here we assume all rings are commutative and modules are *finitely generated*. Let $K$ be a local or global field of zero characteristic and $\mathcal{O}_K$ its ring of integers.

Suppose $L$ is a finite dimensional separable $K$-algebra. An $\mathcal{O}_K$-algebra $\Lambda$ is called an $\mathcal{O}_K$*-order* (in $L$) if it is a finitely generated projective $\mathcal{O}_K$-module (and $\Lambda \otimes_{\mathcal{O}_K} K = L$). A $\mathbf{Z}$-order is simply called an *order*. Let $\Lambda$ be an $\mathcal{O}_K$-order in $L$. We denote the unique maximal $\mathcal{O}_K$-order in $L$ by $\mathcal{O}_L$. If $M$ is a $\Lambda$-module which is projective over $\mathcal{O}_K$, then $M$ is called a $\Lambda$*-lattice*.

For any prime $\wp$ of $\mathcal{O}_K$, we denote by $(\mathcal{O}_K)_\wp, \Lambda_\wp, M_\wp$ their $\wp$-adic completions, respectively. If $K = \mathbf{Q}$ and $\wp = l$ for some prime number $l$, then we write $(\mathcal{O}_K)_l, \Lambda_l, M_l$ for their $l$-adic completions.

A $\Lambda$-module $M$ is called *torsion-free* if $\alpha m \neq 0$ for any non-zerodivisor $\alpha \in \Lambda - \{0\}$ and $m \in M - \{0\}$. In particular, when $\Lambda$ is a domain then this is equivalent to the standard definition. A $\mathcal{O}_K$-module is projective if and only if it is torsion-free [4, II.4 (4.1)]. So $M$ is a torsion-free $\Lambda$-module if and only if it is a $\Lambda$-lattice. If $M$ is a torsion-free $\Lambda$-module, then it is torsion-free over $\mathcal{O}_K$, hence there is a natural embedding $M \hookrightarrow M \otimes_{\mathcal{O}_K} K$, where $M \otimes_{\mathcal{O}_K} K$ has a natural $L$-module structure. If $M \otimes_{\mathcal{O}_K} K$ is free of rank $e$ over $L$ for some integer $e$, then $M$ is said of *rank* $e$. We shall note here that $e$ is used to denote an arbitrary positive integer in this section.

Suppose $M'$ and $M''$ are any torsion-free $\mathcal{O}_K$-modules with $M' \otimes_{\mathcal{O}_K} K = M'' \otimes_{\mathcal{O}_K} K$, then the *ideal index* $[M'' : M']$ is defined to be the fractional $\mathcal{O}_K$-ideal generated by all determinants of the $K$-linear maps $M'' \otimes_{\mathcal{O}_K} K \xrightarrow{\eta} M' \otimes_{\mathcal{O}_K} K$ such that $\eta(M'') \subseteq M'$. It is an integral $\mathcal{O}_K$-ideal, that is, $[M'' : M'] \subseteq \mathcal{O}_K$, if and only if $M' \subseteq M''$. Let $\mathrm{Tr}_{L/K}$ denote the trace map from $L$ to $K$. Denote the trace dual (also known as the complementary module in

[7]) of $\Lambda$ by $\Lambda^\dagger = \{a \in L \mid \mathrm{Tr}_{L/K}(a\Lambda) \subseteq \mathcal{O}_K\}$. It is easy to see that $\Lambda^\dagger$ is a fractional ideal of $\Lambda$, and $\Lambda \subseteq \Lambda^\dagger$. Define the discriminant (ideal) of $\Lambda$ over $\mathcal{O}_K$ by $\Delta_{\Lambda/\mathcal{O}_K} = [\Lambda^\dagger : \Lambda]$. Note that $\Lambda \subseteq \mathcal{O}_L \subseteq \mathcal{O}_L^\dagger \subseteq \Lambda^\dagger$ and $[\Lambda^\dagger : \mathcal{O}_L^\dagger] = [\mathcal{O}_L : \Lambda]$. The discriminant of $L$ over $K$ is defined by $\Delta_{L/K} = \Delta_{\mathcal{O}_L/\mathcal{O}_K} = [\mathcal{O}_L^\dagger : \mathcal{O}_L]$ and so $[\mathcal{O}_L : \Lambda]^2\, \Delta_{L/K} = \Delta_{\Lambda/\mathcal{O}_K}$. Therefore, the relationship between the ideal index of $\Lambda$ in $\mathcal{O}_L$ and the discriminant of $\Lambda$ is $[\mathcal{O}_L : \Lambda]^2 \mid \Delta_{\Lambda/\mathcal{O}_K}$.

Suppose $L$ is a finite field extension of $K$. Let $\alpha$ be an integral element in $L$ and $h \in \mathcal{O}_K[X]$ be its (monic) minimal polynomial. Let $\Lambda = \mathcal{O}_K[\alpha]$. Then $\Delta_{\Lambda/\mathcal{O}_K} = \mathcal{O}_K\, \Delta(h)$. Let $\wp$ be any non-zero prime ideal of $\mathcal{O}_K$. Then $\Lambda_\wp$ is semisimple and $\Lambda_\wp \cong \prod_{Q\mid\wp} \Lambda_\wp$ where the product ranges over all prime ideals $Q$ of $\Lambda$ lying over $\wp$. There is a bijective correspondence between these $Q$'s of $\Lambda$ and the set of (monic) irreducible factors $\bar{h}_0$ of $\bar{h} = (h \bmod \wp) \in (\mathcal{O}_K/\wp)[X]$. (See [7, Chapter I, Proposition 25, page 27].) If $Q$ corresponds to $\bar{h}_0$ in this bijection, then $Q = (\wp, h_0(\alpha))$ in $\Lambda$. We use the following notation throughout this paper: for any prime ideal $v$ of $\mathcal{O}_L$ lying over a prime $\wp$ of $\mathcal{O}_K$, let $\gamma(v/\wp)$, $\kappa(v/\wp)$ and $\varrho(v/\wp)$ denote the *ramification index*, *residue field degree* and *decomposition degree*, respectively. In particular, when $\Lambda = \mathcal{O}_L$ then $\kappa(Q/\wp) = \dim_{\mathcal{O}_K/\wp} \Lambda/Q = \deg(\bar{h}_0)$ and $\gamma(Q/\wp)$ equals the multiplicity of $\bar{h}_0$ as a factor of $\bar{h}$. We have the following lemma whose proof is due to Hendrik Lenstra.

**Lemma 2.1.** *Let the notation be as above. Then $Q$ is not invertible if and only if $\bar{h}_0^{\,2} \mid \bar{h}$ and all coefficients of the remainder of $h$ upon division by $h_0$ are in $\wp^2$. The $(\mathcal{O}_K)_\wp$-order $\Lambda_\wp$ is not the maximal order if and only if there is a monic irreducible factor $\bar{h}_0$ of $\bar{h}$ such that $\bar{h}_0^{\,2} \mid \bar{h}$, and all coefficients of the remainder of $h$ upon division by $h_0$ are in $\wp^2$.*

*Proof.* Write $J := (\wp, h_0(X))$ in $\mathcal{O}_K[X]$, it is a prime ideal. Then the natural surjective map $\mathcal{O}_K[X] \to \Lambda$ induces a surjective map $\theta : J/J^2 \to Q/Q^2$ with $\mathrm{Ker}(\theta)$ generated by $h$. Write $h$ in base $h_0$ and obtain $h = r_2 h_0^2 + r_1 h_0 + r_0$ for some $r_2, r_1, r_0 \in \mathcal{O}_K[X]$ with $\deg(r_1), \deg(r_0) < \deg(\bar{h}_0)$. Then $h \in J$ if and only if $r_0 \in \wp[X]$, while $h \in J^2$ if and only if $r_1 \in \wp[X]$ and $r_0 \in \wp^2[X]$. So $\dim_{\Lambda/Q} J/J^2 = 1 + \dim_{\mathcal{O}_K/\wp} \wp/\wp^2 = 2$ and hence $\dim_{\Lambda/Q} Q/Q^2 = \dim_{\Lambda/Q} J/J^2 - \dim_{\Lambda/Q} \mathrm{Ker}(\theta) = 2 - \dim_{\Lambda/Q} \mathrm{Ker}(\theta)$, where $\dim_{\Lambda/Q} \mathrm{Ker}(\theta)$ is 0 or 1. Therefore, $\dim_{\Lambda/Q} Q/Q^2 \neq 1$ if and only if $h \in J^2$. We conclude that $Q$ is not invertible if and only if $h \in J^2$, which is equivalent to $\bar{h}_0^{\,2} \mid \bar{h}$ and all coefficients of the remainder of $h$ upon division by $h_0$ are in $\wp^2$. Thus the semilocal ring $\Lambda_\wp$ is maximal if and only if $\Lambda_Q$ is maximal for each prime ideal $Q$ over $\wp$, which is equivalent to $Q$ is invertible, and so follows our assertion. $\square$

**Corollary 2.2.** *Let the notation be as in Lemma 2.1. If $h_0 = X - \beta$ with $\beta \in \mathcal{O}_K$, then $Q$ is not invertible if and only if $h(\beta) \equiv 0 \bmod \wp^2$ and $h'(\beta) \equiv 0 \bmod \wp$, where $h'$ denotes the derivative of $h$.*

*Proof.* The condition $\bar{h}_0^{\,2} \mid \bar{h}$ is equivalent to that $h(\beta) \equiv 0 \bmod \wp$ and $h'(\beta) \equiv 0 \bmod \wp$. The condition that all coefficients of the remainder of $h$ upon division by $h_0$ are in $\wp^2$ is equivalent to $h(\beta) \equiv 0 \bmod \wp^2$. $\square$

The following is an easy exercise in algebraic number theory and so we leave its proof to the reader. In this paper $(\frac{\cdot}{p})$ denotes the Jacobi symbol.

**Lemma 2.3.** *Let $p$ be a prime number in $\mathbf{Z}$ and $m$ a positive integer. Then*

*(1)* $\Delta_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}} = p$ *if* $p \equiv 1 \bmod 4$ *while* $\Delta_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}} = 4p$ *if* $p \not\equiv 1 \bmod 4$*;*

*(2)* $\sqrt{p} \in \mathbf{Q}(\zeta_m)$ *if and only if* $\Delta_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}} \mid m$*;*

*(3) let* $p \neq 2$*, if* $p \mid m$ *then* $\mathbf{Q}(\sqrt{(\frac{-1}{p})p}) \in \mathbf{Q}(\zeta_m)$.

## 2.2 Bass orders

A reference for concepts in this subsection is [2, Chapter 4]. We call an $\mathcal{O}_K$-order $\Lambda$ a *Gorenstein order* if every exact sequence of $\Lambda$-modules $0 \to \Lambda \to M \to N \to 0$, in which $M$ and $N$ are $\Lambda$-lattices is split over $\Lambda$. If $\Lambda$ has the additional property that every $\mathcal{O}_K$-order in $L$ containing $\Lambda$ is also a Gorenstein order, then we call $\Lambda$ a *Bass order*. Note that being a Bass order is a local property, in other words, $\Lambda$ is a Bass $\mathcal{O}_K$-order if and only if $\Lambda_\wp$ is a Bass $(\mathcal{O}_K)_\wp$-order for every prime $\wp$ in $\mathcal{O}_K$.

**Proposition 2.4.** *The following are equivalent:*

*(1)* $\Lambda$ *is a Bass* $\mathcal{O}_K$*-order;*

*(2)* $\mathcal{O}_L/\Lambda$ *is a cyclic* $\Lambda$*-module;*

*(3) every ideal of* $\Lambda$ *can be generated by two elements;*

*(4) for every maximal ideal* $Q$ *of* $\Lambda$ *we have* $\dim_{\Lambda_Q/Q\Lambda_Q}(\mathcal{O}_L)_Q/Q(\mathcal{O}_L)_Q \leq 2$*;*

*(5) the multiplicity of* $\Lambda$ *at each maximal ideal* $Q$ *is* $\leq 2$.

*Proof.* The first three parts are equivalent according to [8, Theorem 2.1]. The last two parts are equivalent to (1) by [5, Theorem 2.1]. □

*Remark 2.5.* Here are some examples of Bass orders of interest.

(i) If $L$ is a quadratic field extension over $K$, then $(\mathcal{O}_L)_\wp/\Lambda_\wp$ is cyclic over $\Lambda_\wp$ for every prime $\wp$ of $\mathcal{O}_K$ and thus $\Lambda$ is a Bass order over $\mathcal{O}_K$.

(ii) All maximal orders in number fields are Bass orders.

We are interested in describing torsion-free modules $M$ over $\Lambda_\wp$ of rank $e$. Recall that $\Lambda_\wp$ is a semilocal ring whose maximal ideals are those prime ideals $Q$ lying over $\wp$, so there is a corresponding decomposition of $M$ as $M \cong \prod_{Q|\wp} M_Q$.

If $\Lambda_\wp = (\mathcal{O}_L)_\wp$, then $M_Q$ is torsion-free over the principal ideal domain $(\mathcal{O}_L)_Q$ of rank $e$, so $M_Q \cong \Lambda_Q^e$ for all $Q$. Thus $M \cong \Lambda_\wp^e$. If $\Lambda_\wp \neq (\mathcal{O}_L)_\wp$, then it is generally hard to classify such modules $M$ in terms of orders in $L_\wp$ (see [2, Chapter 3]). However, torsion-free modules over Bass orders can be described as follows.

**Theorem 2.6 (Bass).** *Let $K$ be a local field, $\mathcal{O}_K$ its ring of integers, and $\Lambda$ a Bass $\mathcal{O}_K$-order in a finite field extension $L$ over $K$. Then every indecomposable torsion-free $\Lambda$-module is a projective $\Lambda'$-module for some $\mathcal{O}_K$-order $\Lambda'$ in $L$ containing $\Lambda$.*

*Proof.* Follows from [2, Theorem (37.13)] and the definition of Bass orders. □

## 2.3 Supersingular $q$-numbers

In this subsection there are the definition of $\mathcal{E}$ and the proof of Lemma 2.8, the latter of which is crucial for the technical part of this paper.

For the rest of the paper $l$ is a prime number different from $p$. Let $\zeta_m = e^{\frac{2\pi\sqrt{-1}}{m}}$ for any positive integer $m$. The primitive $m$-th roots of unity are the $\zeta_m^\nu$ with positive integers $\nu$ that are coprime to $m$. We write $\Phi_m(\cdot)$ for the $m$-th cyclotomic polynomial, i.e., the minimal polynomial of $\zeta_m$.

An algebraic number $\alpha \in \mathbf{C}$ is called a *supersingular $q$-number* if it is of the form $\zeta\sqrt{q}$. Let $\pi = \zeta_m^\nu\sqrt{q}$. Let $K = \mathbf{Q}(\pi^2)$ and let $\mathcal{O}, \mathcal{O}_K$ be the ring of integers of $\mathbf{Q}(\pi), K$, respectively. Obviously $K = \mathbf{Q}(\zeta_{m/(2,m)})$ and $[\mathbf{Q}(\pi) : K] = 1$ or 2. (In this paper $(m_1, m_2) := gcd(m_1, m_2)$ for any integer $m_1, m_2$.)

**Lemma 2.7.** *Suppose $q$ is a non-square. Then $\mathbf{Q}(\pi) = K$ if and only if*

$$(1)\ \Delta_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}} \mid m, \quad \textit{and} \quad (2)\ \Delta_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}} \nmid m/(2,m)\ \textit{if}\ 4 \mid m.$$

*In this case $2 \mid \gamma(v/p)$ for any prime $v$ of $\mathcal{O}$ lying over $p$.*

*Proof.* We note $\mathbf{Q}(\pi) = \mathbf{Q}\left(\zeta_{m/(2,m)}, \sqrt{p\zeta_{m/(2,m)}}\right) = K\left(\sqrt{p\zeta_{m/(2,m)}}\right)$. Thus $\mathbf{Q}(\pi) = K$ if and only if $\sqrt{p\zeta_{m/(2,m)}} \in K$, and if and only if

$$K(\sqrt{p}) = K\left(\sqrt{\zeta_{m/(2,m)}}\right),$$

that is, $\mathbf{Q}\left(\zeta_{m/(2,m)}, \sqrt{p}\right) = \mathbf{Q}(\zeta_m)$. This is equivalent to

$$(1a)\ \sqrt{p} \in \mathbf{Q}(\zeta_m), \quad \text{and} \quad (2a)\ \sqrt{p} \notin \mathbf{Q}(\zeta_{m/(2,m)})\ \text{if}\ 4 \mid m,$$

which is equivalent to (1) and (2) respectively by Lemma 2.3 (2).

To show the second assertion it is enough to prove it for just one prime $v$ over $p$ since all primes lying over $p$ are conjugate as $\mathbf{Q}(\pi)$ is the cyclotomic field $\mathbf{Q}(\zeta_{m/(2,m)})$. We claim $(2,p)p \mid \frac{m}{(2,m)}$. In fact, if $p = 2$ then (1) implies $8 \mid m$ by Lemma 2.3 (1) so our claim follows; if $p \neq 2$ then (1) implies $p \mid m$. But since $p \neq 2$, we have $(2,p)p \mid \frac{m}{(2,m)}$. By Lemma 2.3 (3), we thus see that $\mathbf{Q}(\zeta_{m/(2,m)})$ contains a quadratic field $\mathbf{Q}(\sqrt{(\frac{-1}{p})p})$ over $\mathbf{Q}$ where $p$ is totally ramified. Hence $2 \mid \gamma(v/p)$. □

For any prime number $l$, let $m_l$ and $m_{(l)}$ denote, respectively, the $l$-part and the non-$l$-part of a positive integer $m$. Let $\mathcal{E}$ be the set of supersingular

$q$-numbers $\zeta_m^\nu \sqrt{q}$ which satisfy the following conditions: $p \neq 2$, $q$ is not a square, $p \nmid m$, and

(1) $4 \nmid m$ when $p \equiv 1 \bmod 4$; and (2) $4 || m$ when $p \equiv 3 \bmod 4$.

We remark here that $\alpha \in \Lambda_\wp$ is a unit if and only if $\alpha$ is coprime to $\wp$.

**Lemma 2.8.** *Let the notation be as above. If $(l, \pi) \notin \{2\} \times \mathcal{E}$ then $\mathbf{Z}[\pi]_l = \mathcal{O}_l$. If $(l, \pi) \in \{2\} \times \mathcal{E}$ then $\mathbf{Z}[\pi]_2 \subsetneq \mathcal{O}_2$; let $\wp$ be any prime in $\mathcal{O}_K$ lying over 2, then*

*(1) $\mathbf{Q}(\pi)$ is a quadratic extension over $K$ where $\wp$ is split if $p \equiv \pm 1 \bmod 8$, and $\wp$ is inert if $p \equiv \pm 3 \bmod 8$.*

*(2) $\mathbf{Z}[\pi]_\wp$ is a local ring and a Bass $(\mathcal{O}_K)_\wp$-order such that $\mathcal{O}_\wp$ is the only $(\mathcal{O}_K)_\wp$-order in $\mathbf{Q}(\pi)_\wp$ that properly contains $\mathbf{Z}[\pi]_\wp$. Moreover, $\mathcal{O}_\wp / \mathbf{Z}[\pi]_\wp \cong_{(\mathcal{O}_K)_\wp} (\mathcal{O}_K)_\wp / \wp$.*

*Proof.* If $q$ is a square, then $\pi \notin \mathcal{E}$ and $\mathbf{Z}[\pi]_l = \mathbf{Z}[\zeta_m]_l = \mathcal{O}_l$. For the rest of the proof, we assume $q$ is not a square. We consider the following two cases.

Case 1. $l \neq 2$ or $p \mid m$.

We claim $\mathbf{Z}[\pi]_l = \mathcal{O}_l$. Since $l \neq p$, we note that $\mathbf{Z}[\pi^2]_l = \mathbf{Z}[\zeta_{m/(2,m)}]_l = (\mathcal{O}_K)_l$. Suppose $l \neq 2$, obviously $\mathbf{Z}[\pi^2]_l = (\mathcal{O}_K)_l \subseteq \mathbf{Z}[\pi]_l \subseteq \mathcal{O}_l$. If $\mathbf{Q}(\pi) = K$ then $\mathcal{O}_l = (\mathcal{O}_K)_l$ and so $\mathbf{Z}[\pi]_l = \mathcal{O}_l$. If $\mathbf{Q}(\pi) \neq K$ then $[\mathcal{O} : \mathbf{Z}[\pi]]_l^2 \mid \Delta_{\mathbf{Z}[\pi]/(\mathcal{O}_K)}$; but since $\mathbf{Z}[\pi] \cong \mathcal{O}_K[X]/(X^2 - q\zeta_{m/(2,m)})$, we have $\Delta_{\mathbf{Z}[\pi]/\mathcal{O}_K} = \mathcal{O}_K \Delta(X^2 - q\zeta^\nu_{m/(2,m)}) = 4q\mathcal{O}_K$. So $(\Delta_{\mathbf{Z}[\pi]/\mathcal{O}_K})_l = (\mathcal{O}_K)_l$ since $4q$ is coprime to $l$. Therefore $[\mathcal{O} : \mathbf{Z}[\pi]]_l$ is the unit ideal and so $\mathbf{Z}[\pi]_l = \mathcal{O}_l$.

Now let $l = 2$ and $p \mid m$. By Lemma 2.3 (3), $\sqrt{(\frac{-1}{p})p} \in \mathbf{Z}[\zeta_{m/(2,m)}]_2 = \mathbf{Z}[\pi^2]_2 \subseteq \mathbf{Z}[\pi]_2$. Moreover, the norm of $\sqrt{(\frac{-1}{p})p}$ over $\mathbf{Q}$ is $\pm p$ which is coprime to 2 so $\sqrt{(\frac{-1}{p})p}$ is a unit in $\mathbf{Z}[\pi]_2$. Therefore, $\mathbf{Z}[\pi]_2 = \mathbf{Z}[\pi\sqrt{(\frac{-1}{p})p}]_2 = \mathbf{Z}[\zeta_m^\nu \sqrt{(\frac{-1}{p})}]_2$. This proves our claim.

Case 2. $l = 2$ and $p \nmid m$.

Write $m = 2^j m_{(2)}$. It is easy to verify that $\mathbf{Q}(\pi) = \mathbf{Q}(\zeta_{m_{(2)}}, \alpha)$ where $\alpha = \zeta_{2^j}^\mu \sqrt{p}$ for some $2^j$-th primitive root of unity $\zeta_{2^j}^\mu$. We note that $\mathbf{Q}(\zeta_{m_{(2)}})$ and $\mathbf{Q}(\alpha)$ are linearly disjoint and that the minimal polynomial of $\alpha$ over $\mathbf{Q}(\zeta_{m_{(2)}})$ is $h = X^{2^{j-1}} + p^{2^{j-2}}$ if $j \geq 2$, and is $h = X^2 - p$ if $j < 2$.

Let $\wp'$ be any prime ideal in the ring of integers of $\mathbf{Q}(\zeta_{m_{(2)}})$ lying over 2. We show $\mathbf{Z}[\pi]_{\wp'} = \mathbf{Z}[\zeta_{m_{(2)}}, \alpha]_{\wp'}$. The inclusion $\mathbf{Z}[\pi]_{\wp'} \subseteq \mathbf{Z}[\zeta_{m_{(2)}}, \alpha]_{\wp'}$ is trivial. Conversely, since $\pi^{2^j} = \zeta_{m_{(2)}}^{2^j} q^{2^{j-1}}$ and $\alpha = \pi \zeta_{m_{(2)}}^{-\mu}$, we have $\zeta_{m_{(2)}}, \alpha \in \mathbf{Z}[\pi]_{\wp'}$. Thus $\mathbf{Z}[\zeta_{m_{(2)}}, \alpha]_{\wp'} \subseteq \mathbf{Z}[\pi]_{\wp'}$. That is, $\mathbf{Z}[\pi]_{\wp'} = \mathbf{Z}[\zeta_{m_{(2)}}, \alpha]_{\wp'}$. Hence, $\mathbf{Z}[\pi]_{\wp'} = (\mathbf{Z}[\zeta_{m_{(2)}}]_{\wp'})[\alpha]$.

If $j \geq 2$, then $h \equiv (X-1)^{2^{j-1}} \bmod \wp'$. Note that $\mathbf{Z}[\zeta_{m_{(2)}}]_{\wp'}$ is a discrete valuation ring, so we have by Corollary 2.2 that $\mathbf{Z}[\pi]_{\wp'}$ is not maximal if and only if $h(1) = 1 + q^{2^{j-2}} \equiv 0 \bmod \wp'^2$, that is, $j = 2$ and $p \equiv 3 \bmod 4$. Similarly, if $j < 2$ then $h \equiv (X-1)^2 \bmod \wp'$ and so $\mathbf{Z}[\pi]_{\wp'}$ is not maximal if and only if $p \equiv 1 \bmod 4$. Note $\mathbf{Z}[\pi]_2 = \prod_{\wp'|2} \mathbf{Z}[\pi]_{\wp'}$. By Lemma 2.1 and the above argument, $\mathbf{Z}[\pi]_2$ is not maximal if and only if $\pi \in \mathcal{E}$.

In the special case $\pi \in \mathcal{E}$, we have $K = \mathbf{Q}(\zeta_{m_{(2)}})$ and $\mathbf{Q}(\pi) = K(\sqrt{(\frac{-1}{p})p})$ is quadratic over $K$. Moreover, $\mathbf{Z}[\pi]_\wp = (\mathcal{O}_K)_\wp[\sqrt{(\frac{-1}{p})p}]$ and $\wp$ is totally ramified in $\mathbf{Z}[\pi]_\wp$. This proves that $\mathbf{Z}[\pi]_\wp$ is a local ring. The decomposition of $\wp$ in the quadratic extension $\mathbf{Q}(\pi)$ over $K$ corresponds to that of 2 in $\mathbf{Q}(\sqrt{(\frac{-1}{p})p})$ over $\mathbf{Q}$, which is as in our assertion. Since $\mathbf{Z}[\pi]_\wp$ is a quadratic order over the complete discrete valuation ring $(\mathcal{O}_K)_\wp$, it is a Bass order by Remark 2.5 (1). As $(\mathcal{O}_K)_\wp$-orders, $\mathbf{Z}[\pi]_\wp \subset \mathcal{O}_\wp \cong (\mathcal{O}_K)_\wp^2$. There is an injection $\mathbf{Z}[\pi]_\wp/(\mathcal{O}_K)_\wp \hookrightarrow \mathcal{O}_\wp/(\mathcal{O}_K)_\wp \cong (\mathcal{O}_K)_\wp$, under which $\mathbf{Z}[\pi]_\wp/(\mathcal{O}_K)_\wp \cong \wp^i(\mathcal{O}_K)_\wp$ for some positive integer $i$. In other words, $\mathbf{Z}[\pi]_\wp = (\mathcal{O}_K)_\wp + \wp^i\mathcal{O}_\wp$ and so $\mathcal{O}_\wp/\mathbf{Z}[\pi]_\wp \cong (\mathcal{O}_K)_\wp/\wp^i$. But $\Delta_{\mathbf{Z}[\pi]_\wp/(\mathcal{O}_K)_\wp} = (\mathcal{O}_K)_\wp\Delta(X^2 - (\frac{-1}{p})p) = 4(\mathcal{O}_K)_\wp$ and hence $[\mathcal{O}_\wp : \mathbf{Z}[\pi]_\wp]^2 = [(\mathcal{O}_K)_\wp : \wp^i]^2 = 2^{2i}(\mathcal{O}_K)_\wp \mid 4(\mathcal{O}_K)_\wp$. Thus $i = 1$, that is, $\mathcal{O}_\wp/\mathbf{Z}[\pi]_\wp \cong (\mathcal{O}_K)_\wp/\wp$ as $(\mathcal{O}_K)_\wp$-modules. Hence $\mathcal{O}_\wp$ is the only $(\mathcal{O}_K)_\wp$-order in $\mathbf{Q}(\pi)_\wp$ that properly contains $\mathbf{Z}[\pi]_\wp$. $\square$

## 2.4 Torsion-free modules over Bass orders

Let the notation be as in section 2.3. For any ring $R$ we use $R^*$ to denote its group of units. Henceforth in this section we assume that $R$ is an order in $\mathbf{Q}(\pi)$ containing $\mathbf{Z}[\pi]$. Let $M$ be a torsion-free $R_l$-modules (as defined in section 2.1) of rank $e$, our goal here is to describe all such modules. We recall that all modules are assumed to be finitely generated.

**Lemma 2.9.** *Let $\wp$ be any prime ideal in $\mathcal{O}_K$ lying over 2. Let $N$ be an indecomposable torsion-free $\mathbf{Z}[\pi]_\wp$-module. Suppose $(l,\pi) \in \{2\} \times \mathcal{E}$. If $\wp$ is inert in $\mathbf{Q}(\pi)$, then $N \cong \mathbf{Z}[\pi]_\wp$ or $\mathcal{O}_\wp$. If $\wp$ is split, i.e., $\wp = \wp_1\wp_2$ for some prime ideals $\wp_1$, $\wp_2$ in $\mathbf{Q}(\pi)$, then $N \cong \mathbf{Z}[\pi]_\wp$, $\mathcal{O}_{\wp_1}$, or $\mathcal{O}_{\wp_2}$.*

*Proof.* By Lemma 2.8, the $\mathbf{Z}[\pi]_\wp$ is a local ring and an $(\mathcal{O}_K)_\wp$-order, so we invoke Theorem 2.6. If $N$ is projective over the local ring $\mathbf{Z}[\pi]_\wp$ then $N \cong \mathbf{Z}[\pi]_\wp$. Otherwise, $N$ is projective over $\mathcal{O}_\wp$. Suppose $\wp$ is inert in $\mathbf{Q}(\pi)$, that is, $\mathcal{O}_\wp$ is a discrete valuation ring then $N \cong_{\mathcal{O}_\wp} \mathcal{O}_\wp$. If $\wp$ splits into $\wp_1$ and $\wp_2$ in $\mathbf{Q}(\pi)$, that is, if $\mathcal{O}_\wp \cong \mathcal{O}_{\wp_1} \times \mathcal{O}_{\wp_2}$, then $N \cong_{\mathcal{O}_\wp} \mathcal{O}_{\wp_1}$ or $\mathcal{O}_{\wp_2}$. Therefore

$$N \cong_{\mathbf{Z}[\pi]_\wp} \mathbf{Z}[\pi]_\wp, \mathcal{O}_{\wp_1}, \text{ or } \quad \mathcal{O}_{\wp_2}.$$

This finishes the proof. $\square$

**Proposition 2.10.** *There is the following isomorphism of $R_l$-modules:*

$$M \cong_{R_l} \begin{cases} R_l^e & \text{if } (l,\pi) \notin \{2\} \times \mathcal{E}, \\ \prod_{\wp|l} (R_\wp^{a_\wp} \times \mathcal{O}_\wp^{b_\wp}) & \text{if } (l,\pi) \in \{2\} \times \mathcal{E} \end{cases}$$

*where $\wp$ ranges over all prime ideals in $\mathcal{O}_K$ lying over 2, and $a_\wp$, $b_\wp$ are non-negative integers such that $a_\wp + b_\wp = e$.*

*Proof.* Suppose $(l,\pi)\notin\{2\}\times\mathcal{E}$. By Lemma 2.8, the $\mathbf{Z}_l$-order $R_l$ is maximal and our assertion follows from the argument preceding Theorem 2.6.

Suppose $(l,\pi)\in\{2\}\times\mathcal{E}$. Since $M_\wp$ is a torsion-free $R_\wp$-module of rank $e$, by the Krull-Schmidt-Azumaya theorem [2, Theorem (30.6)], $M_\wp$ can be expressed as a finite direct sum of indecomposables with the summands unique up to isomorphism and order of occurrence. If $\wp$ is inert in $\mathbf{Q}(\pi)$, then by Lemma 2.9 there are non-negative integers $a_\wp, b_\wp$ with $a_\wp+b_\wp=e$ such that $M_\wp\cong R_\wp^{a_\wp}\times\mathcal{O}_\wp^{b_\wp}$. Now suppose $\wp$ is split in $\mathbf{Q}(\pi)$. Then $M_\wp\cong R_\wp^{a_\wp}\times\mathcal{O}_{\wp_1}^{b_\wp}\times\mathcal{O}_{\wp_2}^{c_\wp}$ for some non-negative integers $a_\wp,b_\wp,c_\wp$; by comparing ranks in $\mathbf{Q}(\pi)_\wp^e\cong_{\mathbf{Q}(\pi)_\wp}\mathbf{Q}(\pi)_\wp^{a_\wp}\times\mathbf{Q}(\pi)_{\wp_1}^{b_\wp}\times\mathbf{Q}(\pi)_{\wp_2}^{c_\wp}$, we are forced to have $b_\wp=c_\wp$. Thus, $M_\wp\cong R_\wp^{a_\wp}\times(\mathcal{O}_{\wp_1}\times\mathcal{O}_{\wp_2})^{b_\wp}\cong R_\wp^{a_\wp}\times\mathcal{O}_\wp^{b_\wp}$ for $a_\wp,b_\wp$ with $a_\wp+b_\wp=e$. Therefore

$$M\cong\prod_{\wp|2}M_\wp\cong_{R_2}\prod_{\wp|2}(R_\wp^{a_\wp}\times\mathcal{O}_\wp^{b_\wp}).$$

This finishes our proof. $\square$

The following corollary is prepared for the next section.

**Corollary 2.11.** *If $M$ is a torsion-free $R_l$-module of rank $e$ then we have $M/(\pi-1)M\cong_{R_l}(R_l/(\pi-1))^e$ unless $l=2$, $q$ is not a square, and $\pi=\pm\sqrt{(\frac{-1}{p})q}$, in which case there are non-negative integers $a,b$ with $a+b=e$ such that*

$$M/(\pi-1)M\cong_{R_2}(R_2/(\pi-1))^a\times(\mathcal{O}_2/(\pi-1))^b.$$

*Proof.* First of all we show that $m\notin 2^{\mathbf{Z}}$ if and only if $R_2/(\pi-1)=0$, that is, $\pi-1\in R_2^*$. Indeed, $m\notin 2^{\mathbf{Z}}$ implies $\zeta_m^\nu-1\in\mathbf{Z}[\pi]_2^*\subseteq R_2^*$. Write $\pi-1=(\zeta_m^\nu-1)\sqrt{q}+(\sqrt{q}-1)$. If $p=2$ then $(\zeta_m^\nu-1)\sqrt{q}$ lies in a prime over 2 while $\sqrt{q}-1\in R_2^*$ so their sum lies in $R_2^*$; if $p\neq 2$, then $R_2^*\sqrt{q}=R_2^*$ and $\sqrt{q}-1$ lies in a prime over 2 thus their sum also lies in $R_2^*$. This proves our claim. Consequently, if $m\in 2^{\mathbf{Z}}$ then $M/(\pi-1)M\cong(R_2/(\pi-1))^e$ since they are both trivial. By Proposition 2.10, we have $M/(\pi-1)M\cong_{R_l}(R_l/(\pi-1))^e$ unless $l=2,\pi\in\mathcal{E}$ and $m\in 2^{\mathbf{Z}}$. By the definition of $\mathcal{E}$, we have $\pi=\zeta_m^\nu\sqrt{q}\in\mathcal{E}$ if and only if $q$ is not a square and $m=1$ or $2$ if $p\equiv 1 \bmod 4$; while $m=4$ if $p\equiv 3\bmod 4$. That is, we have $l=2$, $q$ is not a square and $\pi=\pm\sqrt{(\frac{-1}{p})q}$. $\square$

# 3 Elementary supersingular abelian varieties

## 3.1 Preliminaries

This section provides some auxiliary results on abelian varieties over finite fields. We shall quote from [9] and [10] without comment.

Recall that $l$ is any prime different from $p$. If $G$ is an abelian group we denote by $G[l^\infty]$ the subgroup of all elements in $G$ whose order is a $l$-power. For every $\mathbf{k}$-isogeny $r:A\to A$, we denote by $A[r]$ the kernel of the induced map on $A(\bar{\mathbf{k}})$ as abelian groups. The $l$-adic Tate module $T_l(A)=\varprojlim_n A[l^n]$ is free of rank $2d$ over $\mathbf{Z}_l$. Since the Frobenius endomorphism $\pi$ acts faithfully on it, $T_l(A)$ is torsion-free $\mathbf{Z}[\pi]_l$-module. $V_l(A) = T_l(A) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$ is a $\mathbf{Q}[\pi]_l$-module. We also know that $\mathbf{Q}[\pi]$ is a semisimple $\mathbf{Q}$-algebra. If the characteristic polynomial of the Frobenius is $f = \prod_{i=1}^{t} g_i^{e_i}$ as in section 1, then

$$\mathbf{Q}[\pi]_l \cong \prod_{i=1}^{t} \mathbf{Q}[\pi]_l/(g_i(\pi)), \quad V_l(A) \cong \prod_{i=1}^{t} (\mathbf{Q}[\pi]_l/(g_i(\pi)))^{e_i}. \tag{1}$$

In particular, if $A$ is elementary so $\mathbf{Q}[\pi]$ is a field, then $V_l(A) \cong \mathbf{Q}(\pi)_l^e$. Thus $T_l(A)$ is a torsion-free module of rank $e$ over any $\mathbf{Z}_l$-order of $\mathbf{Q}(\pi)_l$ containing $\mathbf{Z}[\pi]_l$.

$T_l$ defines a (covariant) functor from the category of abelian varieties $A'$ over $\mathbf{k}$ with a $\mathbf{k}$-isogeny $r : A \to A'$ to the category of $\mathbf{Z}[\pi]_l$-modules $T_l(A')$ with an injective $\mathbf{Z}[\pi]_l$-module homomorphism $T_l(A) \to T_l(A')$. For each positive integer $n$ we have $l^{-n}T_l(A)/T_l(A) \cong A[l^n]$ and so, taking direct limits, $V_l(A)/T_l(A) \cong A[l^\infty]$. Mapping the exact sequence $0 \to T_l(A) \to V_l(A) \to A[l^\infty] \to 0$ to that of $A'$ by $r$ induces an injective $\mathbf{Z}[\pi]_l$-module homomorphism $r : T_l(A) \to T_l(A')$ with cokernel $T_l(A')/rT_l(A)$ and an isomorphism $r : V_l(A) \to V_l(A')$. Let $r^{-1}T_l(A')$ be the pullback of $T_l(A') \subset V_l(A')$ under this isomorphism, there is an isomorphism $T_l(A')/rT_l(A) \cong r^{-1}T_l(A')/T_l(A)$. By applying the Snake Lemma to the above resulting diagram, we have $\mathrm{Ker}(r)[l^\infty] \cong r^{-1}T_l(A')/T_l(A)$. In fact, every $\mathbf{Z}[\pi]_l$-lattice (as $\mathbf{Z}_l$-order) of $V_l(A)$ containing $T_l(A)$ arises in this way:

**Proposition 3.1.** *Let $\theta : V_l(A)/T_l(A) \xrightarrow{\sim} A[l^\infty]$ be the isomorphism as above. For every $\mathbf{Z}[\pi]_l$-lattice $M$ containing $T_l(A)$, there is an abelian variety $A'$ with a $\mathbf{k}$-isogeny $r : A \to A'$ such that $M = r^{-1}T_l(A')$ in $V_l(A)$ and $\theta(M/T_l(A)) = \mathrm{Ker}(r)(\bar{\mathbf{k}})$.*

*Proof.* Write $G = \theta(M/T_l(A))$, it is a finite subgroup of $A[l^\infty]$. By our assumption, there is an étale subgroup scheme $\mathcal{G}$ of $A$ over $\mathbf{k}$ with $\mathcal{G}(\bar{\mathbf{k}}) = G$. Take $A' = A/\mathcal{G}$ and the $\mathbf{k}$-isogeny $r : A \to A'$ with $\mathrm{Ker}(r) = \mathcal{G}$. The argument preceding the proposition indicates $\theta(r^{-1}T_l(A')/T_l(A)) = \mathcal{G}[l^\infty] = G$. □

Define $T_p(A) = \varprojlim_n A[p^n]$ in an analogous manner. It is free $\mathbf{Z}_p$-module of rank between 0 and $d$ (inclusive).

**Proposition 3.2.** *For any $\mathbf{k}$-isogeny $r : A \to A$, there is an isomorphism of abelian groups:*

$$A[r] \cong \prod_l T_l(A)/rT_l(A)$$

*where $l$ ranges over all prime numbers.*

*Proof.* The finite abelian group $A[r]$ has the decomposition $A[r] \cong \prod_l (A[r])[l^\infty]$, where each component is isomorphic to $T_l(A)/rT_l(A)$. □

Note that $A(\mathbf{k}) = A[\pi - 1]$.

### 3.2 Elementary supersingular abelian varieties

An abelian variety over $\mathbf{k}$ is supersingular if and only if the eigenvalues of its Frobenius $\pi$ are supersingular $q$-numbers. This is equivalent to that the Newton polygon of $A$ is a straight line of slope $1/2$, which is equivalent to that $A$ is $\bar{\mathbf{k}}$-isogenous to a power of a supersingular elliptic curve (as a special case of [11, Theorem 4.2]). A supersingular abelian variety $A$ over $\mathbf{k}$ has $A[p]=0$. We remark in brief that the converse is not true when $d>2$. In fact, an abelian variety has $A[p]=0$ if and only if its Newton polygon has no 0-slope segment, which does not imply being a straight line of slope $1/2$ when $d>2$.

For the rest of this section we assume that $A$ is an elementary supersingular abelian variety over $\mathbf{k}$ whose Frobenius relative to $\mathbf{k}$ is $f=g^e$ for some monic irreducible polynomial $g$ over $\mathbf{Q}$ and a positive integer $e$.

Since $\mathbf{Q}[\pi]=\mathbf{Q}(\pi)$ is a field, we fix an embedding of $\mathbf{Q}(\pi)$ in $\mathbf{C}$ and identifying $\pi$ with its image, we write $\pi=\zeta_m^\nu\sqrt{q}$ for some primitive $m$-th root of unity $\zeta_m^\nu$. We resume the notation from section 2.3: $K=\mathbf{Q}(\pi^2)=\mathbf{Q}(\zeta_{m/(2,m)})$, its ring of integers $\mathcal{O}_K=\mathbf{Z}[\zeta_{m/(2,m)}]$, and $\mathcal{O}$ the ring of integers of $\mathbf{Q}(\pi)$.

Let $\mathcal{Q}$ be the set of all supersingular $q$-numbers $\zeta_m^\nu\sqrt{q}$ for some primitive root of unity $\zeta_m^\nu$ such that either of the following two conditions is satisfied: (1) $m=1$ or $2$; (2) $q$ is a square, $(2,p)p\nmid m$ and $p$ is of odd order in the group $(\mathbf{Z}/m_{(p)}\mathbf{Z})^*$.

**Proposition 3.3.** *Suppose $A$ is simple supersingular over $\mathbf{k}$.*

*(1) When $\pi\in\mathcal{Q}$ then $e=2$ and $\mathrm{End}^0_{\mathbf{k}}(A)$ is a quaternion algebra over $\mathbf{Q}(\pi)$;*

*(2) When $\pi\notin\mathcal{Q}$ then $e=1$ and $\mathrm{End}^0_{\mathbf{k}}(A)$ is commutative and equal to $\mathbf{Q}(\pi)$.*

*Proof.* Let $v$ be any place of $\mathbf{Q}(\pi)$ (including both finite and infinite primes). Let $e_v$ denote the denominator of the Hasse invariant, $\mathrm{inv}_v(\mathrm{End}^0_{\mathbf{k}}(A))$, of $\mathrm{End}^0_{\mathbf{k}}(A)$ at $v$. By [14, Théorème 1] we have

$$\mathrm{inv}_v(\mathrm{End}^0_{\mathbf{k}}(A))=\frac{\mathrm{ord}_v(\pi)[\mathbf{Q}(\pi)_v:\mathbf{Q}_p]}{\mathrm{ord}_v(q)}=\frac{[\mathbf{Q}(\pi)_v:\mathbf{Q}_p]}{2}=\frac{\gamma(v/p)\kappa(v/p)}{2}\bmod 1,$$

for all primes $v$ lying over $p$, so $e_v=1$ or $2$. Now $e_v=1$ for all complex $v$ and also for all finite primes $v$ not lying over $p$, while $e_v=2$ for all real $v$. We have $e=\mathrm{lcm}_v(e_v)=2$ if either (1)' $v$ is real or (2)' $\gamma(v/\wp)\kappa(v/\wp)$ is odd; and $e=1$ otherwise. It is obvious that (1)' is equivalent to (1). We show below that if $v$ is not real prime then (2)' is equivalent to (2):

Suppose $q$ is not a square: we claim that $e_v=1$ for all finite primes $v$ over $p$. Now $[\mathbf{Q}(\pi):K]=1$ or $2$. The former implies $2\mid\gamma(v/p)$. Consider the latter case, if $\sqrt{p}\in\mathbf{Q}(\pi)$, then $2\mid\gamma(v/p)$ and so $e_v=1$; otherwise, we would have quadratic extensions $\mathbf{Q}(\zeta_m,\sqrt{p})\supset\mathbf{Q}(\pi)\supset K$. But if $p$ was unramified in $\mathbf{Q}(\pi)/K$, then it would be unramified in $\mathbf{Q}(\zeta_m,\sqrt{p})/\mathbf{Q}(\zeta_m)$, which is absurd; so we must conclude that $p$ is totally ramified in $\mathbf{Q}(\pi)/K$ and hence $2\mid\gamma(v/p)$ and so $e_v=1$.

Suppose $q$ is a square: so that $\mathbf{Q}(\pi)=\mathbf{Q}(\zeta_m)$. Then for any finite prime $v$ over $p$, we have that $\kappa(v/p)$ equals the order of $p$ in $(\mathbf{Z}/m_{(p)}\mathbf{Z})^*$; Let $\phi(\cdot)$ denote the Euler phi-function here, then $\gamma(v/p) = \phi(m_p)$, which is odd if and only if $(2,p)p \nmid m$. This finishes our proof. $\square$

*Remark 3.4.* Suppose $A$ is simple supersingular over $\mathbf{k}$. If $\pi \in \mathcal{E}$, then $\pi \in \mathcal{Q}$ if and only if $d = 2$. This follows from the above proposition and the definitions of $\mathcal{E}$ and $\mathcal{Q}$.

*Remark 3.5.* Let $A$ be a simple supersingular abelian variety with odd dimension $d > 2$, then $e = 1$ and $\mathrm{End}^0_{\mathbf{k}}(A)$ must be commutative. Indeed, recall [14, Théorème 1] that $2d = e[\mathbf{Q}(\pi) : \mathbf{Q}]$ and so it suffices to show $2 \mid [\mathbf{Q}(\pi) : K][\mathbf{Q}(\zeta_{m/(2,m)}) : \mathbf{Q}]$. Either $[\mathbf{Q}(\pi) : K] = 1$ or 2, in the former case $[\mathbf{Q}(\zeta_{m/(2,m)}) : \mathbf{Q}] = \phi(m/(2,m)) > 1$ and so is even.

## 3.3 Module structures

Let $R$ be a subring in $\mathbf{Q}(\pi)$ with $\mathbf{Z}[\pi] \subseteq R \subseteq \mathrm{End}_{\mathbf{k}}(A) \cap \mathbf{Q}(\pi)$. For any finite group $G$, we write $\#G$ for its order.

**Lemma 3.6.** *Let $M' \subseteq M''$ be modules over any ring $R$. Let $r \in R$ be such that $rR$ is of finite index in $R$ and $r$ acts faithfully on $M', M''$.*

*(1) If $M'$ contains a free $R$-module of rank $s$ as a submodule of finite index, then*
$$\#M'/rM' = (\#(R/rR))^s.$$

*(2) If $M', M''$ contain a free $R$-module of rank $s$ as a submodule of finite index in $M', M''$, respectively, then there are homomorphisms $\rho' : M'/rM' \to M''/rM''$ and $\rho'' : M''/rM'' \to M'/rM'$ with*
$$\#\mathrm{Ker}(\rho') = \#\mathrm{Coker}(\rho') = \#\mathrm{Ker}(\rho'') = \#\mathrm{Coker}(\rho'') \mid \#M''/M'.$$

*Proof.* (1) Since $r$ acts faithfully on $M'$ and $R^s$, the injective map $r : M' \to M'$ induces an injective map $r : R^s \hookrightarrow R^s$. On the other hand, the given injection $R^s \hookrightarrow M'$ is of finite index, we thus have
$$\#(M'/rM') \cdot \#(M'/R^s) = \#(R^s/rR^s) \cdot \#(M'/R^s).$$
Therefore, $\#M'/rM' = \#(R/rR)^s$.

(2) Let $r$ act on the short exact sequence of $R$-modules
$$0 \to M' \to M'' \to M''/M' \to 0,$$
and apply the Snake lemma. We then get the desired map $\rho'$ with $\#\mathrm{Coker}(\rho')$ dividing $\#M''/M'$. By part (1), we have $\#M'/rM' = \#M''/rM''$ as they both equal $\#(R/rR)^s$. Thus $\#\mathrm{Ker}(\rho') = \#\mathrm{Coker}(\rho')$. Any finite $R/rR$-module $N$ has an isomorphic dual $\mathrm{Hom}_{\mathbf{Z}}(N, \mathbf{Q}/\mathbf{Z})$, our assertion on $\rho''$ follows by taking the dual of $\rho'$. $\square$

**Proposition 3.7.** *Let $r$ be an isogeny in $R$. Then there is an $R$-module homomorphism*

$$\varphi_r : A[r] \longrightarrow \prod_{l\neq p}(R_l/rR_l)^e$$

*which is an isomorphism except when $\pi \in \mathcal{E}$ in which case $\#\mathrm{Ker}(\varphi_r)$ and $\#\mathrm{Coker}(\varphi_r)$ are equal and divide $2^d_{(p)}$.*

*Proof.* By Proposition 3.2 and the fact $A[p] = 0$, we have $A[r] \cong \prod_{l\neq p} T_l/rT_l$. Recall that $T_l$ is a torsion-free $R_l$-module of rank $e$, so we invoke Proposition 2.10. If $\pi \notin \mathcal{E}$ or $p = 2$, then $T_l/rT_l \xrightarrow{\sim} (R_l/rR_l)^e$ for each $l \neq p$, and we obtain the desired isomophism $\varphi_r$. Now suppose $\pi \in \mathcal{E}$. Lemma 2.8 (2) implies $\#\mathcal{O}_\wp/R_\wp \mid \#\mathcal{O}_\wp/\mathbf{Z}[\pi]_\wp = \#(\mathcal{O}_K)_\wp/\wp = 2^{\kappa(\wp/2)}$. Clearly $\kappa(\wp/2)\varrho(\wp/2) \mid [K:\mathbf{Q}]$ and $[K:\mathbf{Q}] = [\mathbf{Q}(\pi):\mathbf{Q}]/2$ by Lemma 2.8 (1). For each $l$, we have a map $T_l/rT_l \to (R_l/rR_l)^e$ which is an isomorphism if $l \neq 2$. When $l = 2$, Lemma 3.6 indicates the size of its kernel and cokernel are equal and divide $(\#T_2/R_2^e)_{(p)}$. Taking product over all $l \neq p$ we obtain the desired map $\varphi_r$ with $\#\mathrm{Ker}(\varphi_r) = \#\mathrm{Coker}(\varphi_r)$ and divides

$$(\#\mathcal{O}_2/R_2)^e_{(p)} \mid 2^{\kappa(\wp/2)\varrho(\wp/2)e}_{(p)} \mid 2^{e[K:\mathbf{Q}]}_{(p)} \mid 2^{e[\mathbf{Q}(\pi):\mathbf{Q}]/2}_{(p)}$$

where the last number equals $2^d_{(p)}$. □

**Proof of Theorem 1.2.** Let $S = \mathbf{Z} - p\mathbf{Z}$. By Proposition 3.7, there is an $R$-module homomorphism $\varphi_n : A[n] \to ((\frac{1}{n}R)/R)^e$ for every $n \in S$. Let $W_n$ be the set of such homomorphisms. If $m \mid n$, then by passing to the largest submodule annihilated by $m$ we see that any $R$-module homomorphism $\varphi_n$ maps the submodule $A[m]$ of $A[n]$ to $((\frac{1}{m})R/R)^e$, so there is a restriction map $W_n \to W_m$. Since the projective limit of a system of non-empty finite sets is non-empty, the projective limit of the sets $W_n$ is non-empty. Therefore we can make a simultaneous choice of $R$-module homomorphisms $\varphi_n$ that commute with the inclusions $A[m] \subseteq A[n]$ and $((\frac{1}{m}R)/R)^e \subseteq ((\frac{1}{n}R)/R)^e$. Taking the injective limit over $n \in S$, we get an $R$-module homomorphism $\varinjlim A[n] \to \varinjlim((\frac{1}{n}R)/R)^e$, that is $\varphi : A(\bar{\mathbf{k}}) \xrightarrow{\sim} (R_{(p)}/R)^e$. Since $A(\bar{\mathbf{k}})$ and $(R_{(p)}/R)^e$ are both divisible as abelian groups, the cokernel of $\varphi$ is also divisible, but it is finite and hence trivial. So $\mathrm{Coker}(\varphi) \cong \varinjlim \mathrm{Coker}(\varphi_n)$ is trivial and $\varphi$ is surjective. In $A(\bar{\mathbf{k}})$ we have $\mathrm{Ker}(\varphi) \cong \varinjlim \mathrm{Ker}(\varphi_n)$. Thus $\varphi$ is an isomorphism except when $\pi \in \mathcal{E}$, in which case $\#\mathrm{Ker}(\varphi)$ divides $2^d_{(p)}$ since $\#\mathrm{Ker}(\varphi_n)$ divides $2^d_{(p)}$ for each $n$. □

**Proposition 3.8.** *Let $A$ be a simple supersingular abelian variety over $\mathbf{k}$ with $f = g^e$. Let $R = \mathrm{End}_{\mathbf{k}}(A) \cap \mathbf{Q}(\pi)$. If $p = 2$ or $d \neq 2$, then $A(\bar{\mathbf{k}}) \cong_R (R_{(p)}/R)^e$. If $p \neq 2$ and $d = 2$, then there are non-negative integers $a, b$ with $a + b = e$ and*

$$A(\bar{\mathbf{k}}) \cong_R (R_{(p)}/R)^a \times (\mathcal{O}_{(p)}/\mathcal{O})^b.$$

*Proof.* Let $\varphi : A(\bar{\mathbf{k}}) \to (R_{(p)}/R)^e$ be defined as in Theorem 1.2, which is an isomorphism unless $\pi \in \mathcal{E}$. Suppose $\pi \in \mathcal{E}$. Then $\#\mathrm{Ker}(\varphi) = \#\mathrm{Coker}(\varphi)$

is a 2-power. Suppose $d \neq 2$. Then $e = 1$ by Remark 3.4 and so $T_2$ is a torsion-free $R_2$-module of rank 1. Recall that $K$ is a cyclotomic field. For any prime $\wp$ in $\mathcal{O}_K$ lying over 2, write $T_\wp$ for the $\wp$-adic completion of $T_2$ and $T_\wp : T_\wp = \{r \in R_\wp \mid rT_\wp \subseteq T_\wp\}$. Then $T_\wp : T_\wp = R_\wp$, so $T_\wp$ is a fractional ideal of $R_\wp$. Recall from Lemma 2.8 that $R_\wp$ is a Bass $(\mathcal{O}_K)_\wp$-order and thus $T_\wp \cong_{R_\wp} R_\wp$ by [1, § 2.6]. So $T_2 \cong_{R_2} R_2$ and this induces isomorphism $T_2/2T_2 \xrightarrow{\sim} R_2/2R_2$ by Lemma 3.6. Thus $\varphi$ is an isomorphism. Suppose $d = 2$. Then $\pi \in \mathcal{E}$ implies $\pi = \pm\sqrt{(\frac{-1}{p})q}$ and $e = 2$ by Remark 3.4. In this case, $\wp = 2$, so by Proposition 2.10, we have $A[n] \cong \prod_{l \neq p} T_l/nT_l \cong (\frac{1}{n}R/R)^a \times (\frac{1}{n}\mathcal{O}/O)^b$ for all $n \in S = \mathbf{Z} - p\mathbf{Z}$. Take injective limit both sides over $n \in S$, we have

$$A(\bar{\mathbf{k}}) \cong \varinjlim((\tfrac{1}{n}R/R)^a \times (\tfrac{1}{n}\mathcal{O}/\mathcal{O})^b) \cong_R (R_{(p)}/R)^a \times (\mathcal{O}_{(p)}/\mathcal{O})^b.$$

This finishes our proof. □

### 3.4 Group structures

In this subsection we shall apply the results of the previous subsection to our study of the group structure of $A(\mathbf{k})$.

If $A$ is exceptional, $\mathbf{Q}(\pi) = \mathbf{Q}(\sqrt{(\frac{-1}{p})q}) = \mathbf{Q}(\sqrt{(\frac{-1}{p})p})$, so $\mathcal{O} = \mathbf{Z}[\frac{1+\sqrt{(\frac{-1}{p})p}}{2}]$. By Lemma 2.8 (2) we notice $\mathcal{O}_2/\mathbf{Z}[\pi]_2 \cong \mathbf{Z}_2/2\mathbf{Z}_2 \cong \mathbf{Z}/2\mathbf{Z}$.

**Proof of Theorem 1.1.** Apply Corollary 2.11 to $M = T_l(A)$ and $R = \mathbf{Z}[\pi]$. Now

$$A(\mathbf{k}) \cong_{\mathbf{Z}[\pi]} (\mathbf{Z}[\pi]/(\pi - 1))^e \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^e$$

unless $A$ is exceptional, in which case the argument preceding the proof implies that $(\pi-1)/2 \in \mathcal{O}_2$ while $(\pi-1)/4 \notin \mathcal{O}_2$. Since $\#\mathcal{O}_2/(\pi-1) = \#\mathbf{Z}[\pi]_2/(\pi-1) = |g(1)|_2$, we have

$$\mathcal{O}_2/(\pi - 1) \cong_{\mathbf{Z}_2} \mathbf{Z}_2/2\mathbf{Z}_2 \times \mathbf{Z}_2/\tfrac{g(1)}{2}\mathbf{Z}_2.$$

Hence there are non-negative integers $a, b$ with $a + b = e$ such that

$$\begin{aligned} A(k) &\cong_{\mathbf{Z}[\pi]} (\mathbf{Z}[\pi]_2/(\pi-1))^a \times (\mathcal{O}_2/(\pi-1))^b \times \textstyle\prod_{l\neq 2}(\mathbf{Z}[\pi]_l/(\pi-1))^e \\ &\cong_{\mathbf{Z}} ((\mathbf{Z}_2/g(1)\mathbf{Z}_2)^a \times (\mathbf{Z}_2/\tfrac{g(1)}{2}\mathbf{Z}_2 \times \mathbf{Z}_2/2\mathbf{Z}_2)^b) \times \textstyle\prod_{l\neq 2}(\mathbf{Z}_l/g(1)\mathbf{Z}_l)^e \\ &\cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^a \times (\mathbf{Z}/\tfrac{g(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})^b. \end{aligned}$$

This proves our theorem. □

**Proposition 3.9.** *Let the notation be as in Theorem 1.1. If $A$ is exceptional, then for every pair of non-negative integers $a', b'$ with $a' + b' = e$ there exists an abelian variety $A'$ isogenous over* $\mathbf{k}$ *to $A$ such that*

$$A'(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^{a'} \times (\mathbf{Z}/\tfrac{g(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})^{b'}.$$

*Proof.* Let $A$ be exceptional. By Theorem 1.1, there are non-negative integers $a, b$ with $a+b=e$ such that $T_2 \cong_{\mathbf{Z}[\pi]_2} \mathbf{Z}[\pi]_2^a \times \mathcal{O}_2^b$ and

$$A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^a \times (\mathbf{Z}/\tfrac{g(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})^b.$$

If $b'=b$, then we are done. If $b'<b$, let

$$M = \mathbf{Z}[\pi]_2^a \times \mathcal{O}_2^{b'} \times (\tfrac{1}{2}\mathbf{Z}[\pi]_2)^{b-b'};$$

if $b'>b$, let

$$M = \mathbf{Z}[\pi]_2^{a'} \times \mathcal{O}_2^{b'},$$

in either case $M \cong_{\mathbf{Z}[\pi]_2} \mathbf{Z}[\pi]_2^{a'} \times \mathcal{O}_2^{b'}$. By the argument preceding the proof of Theorem 1.1, we know that $\mathcal{O}_2 \subseteq \frac{1}{2}\mathbf{Z}[\pi]_2 \subset \mathbf{Q}(\pi)_2$. By Proposition 3.1, there exits an abelian variety $A'$ over $\mathbf{k}$ with $T_2(A')=M$ and a $\mathbf{k}$-isogeny $A \xrightarrow{r} A'$ with $\mathrm{Ker}(r)(\bar{\mathbf{k}}) \cong T_2(A')/T_2(A)$ while $T_l(A')=T_l(A)$ for all $l \neq 2$. Thus

$$\begin{aligned} A'(\mathbf{k}) &\cong \quad \textstyle\prod_{l\neq p} T_l(A')/(\pi-1)T_l(A') \\ &\cong_{\mathbf{Z}[\pi]} (\mathbf{Z}_2[\pi]/(\pi-1))^{a'} \times (\mathcal{O}_2/(\pi-1))^{b'} \times \textstyle\prod_{l\neq 2}(\mathbf{Z}[\pi]_l/(\pi-1))^e \\ &\cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^{a'} \times (\mathbf{Z}/\tfrac{g(1)}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})^{b'}. \end{aligned}$$

This finishes the proof. □

**Corollary 3.10.** *Suppose $A$ is a simple supersingular abelian variety over $\mathbf{k}$ of dimension $d>2$ with $f=g^e$, then $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^e$ with $e=1$ or 2. If $d=1$ or 2 then $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^e$ or $A(\mathbf{k}) \cong_{\mathbf{Z}} \mathbf{Z}/\frac{q+1}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.*

*Proof.* If $A$ is simple over $\mathbf{k}$ of dimension $d>2$, then $A$ is never exceptional, so $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^e$, where $e=1$ or 2 as we have seen in Proposition 3.3.

If $A$ is an elliptic curve, then $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^e$ unless $A$ is exceptional in which case $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^e$ or $A(\mathbf{k}) \cong_{\mathbf{Z}} \mathbf{Z}/\frac{q+1}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Both cases may occur because of Proposition 3.9. (This result can be found in [12, Chapter 4].)

If $A$ is of dimension 2, then $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^2$ unless $A$ is exceptional in which case $A(\mathbf{k}) \cong_{\mathbf{Z}} (\mathbf{Z}/g(1)\mathbf{Z})^2$ or $A(\mathbf{k}) \cong_{\mathbf{Z}} \mathbf{Z}/\frac{q-1}{2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Both cases may occur because of Proposition 3.9. □

In particular, by Remark 3.5, if $A$ is simple supersingular of odd dimension $d>2$, then $A(\mathbf{k}) \cong \mathbf{Z}/g(1)\mathbf{Z}$ is cyclic.

# References


[1] J. Buchmann and H.W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260.

[2] C.W. Curtis and I. Reiner, *Methods of representation theory*, vol. 1, J. Wiley and Sons, 1990.

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

[4] A. Frohlich and M.J. Taylor, *Algebraic number theory*, Cambridge studies in advanced mathematics, vol. 27, Cambridge University Press, 1991.

[5] C. Greither, *On the two generator problem for the ideals of a one-dimensional ring*, J. Pure Appl. Algebra **24** (1982), 265–276.

[6] H.W. Lenstra, Jr., *Complex multiplication structure of elliptic curves*, J. Number Theory **56** (1996), 227–241.

[7] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, Springer-Verlag, 1986.

[8] L. Levy and R. Wiegand, *Dedekind-like behavior of rings with* 2*-generators*, J. Pure Appl. Algebra **37** (1985), 41–58.

[9] J. Milne, *Abelian varieties*, Arithmetic geometry (G. Cornell and J. Silverman, eds.), Springer-Verlag, 1987.

[10] D. Mumford, *Abelian varieties*, Oxford University Press, 1974.

[11] F. Oort, *Subvarieties of moduli spaces*, Invent. Math. **24** (1974), 95–119.

[12] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory. Ser. A **46** (1987), 183–211.

[13] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.

[14] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki **21** (1968/69), no. 352, 95–110.

[15] W. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **2** (1969), 521–560.

[16] W. Waterhouse and J. Milne, *Abelian varieties over finite fields*, Proc. Sympos. Pure Math. **20** (1971), 53–64.

[17] C-P. Xing, *On supersingular abelian varieties of dimension two over finite fields*, Finite Fields Appl. **2** (1996), 407–421.

[18] H. Zhu, *Supersingular abelian varieties over finite fields*, Preprint.