ENDOMORPHISMS OF ORDINARY SUPERELLIPTIC JACOBIANS

YURI G. ZARHIN

Abstract. Let $K$ be a field of prime characteristic $p$, $n \geq 5$ an integer, $f(x)$ an irreducible polynomial over $K$ of degree $n$, whose Galois group is either the full symmetric group $S_n$ or the alternating group $A_n$. Let $\ell$ be an odd prime different from $p$, $\mathbb{Z}[\zeta_\ell]$ the ring of integers in the $\ell$th cyclotomic field, $C_{f,\ell} : y^\ell = f(x)$ the corresponding superelliptic curve and $J(C_{f,\ell})$ its jacobian. We prove that the ring of all endomorphisms of $J(C_{f,\ell})$ coincides with $\mathbb{Z}[\zeta_\ell]$ if $J(C_{f,\ell})$ is an ordinary abelian variety and $(\ell, n) \neq (5, 5)$.

2000 Math. Subj. Class: Primary 14H40; Secondary 14K05, 11G 30, 11G10

Key words and phrases: ordinary abelian varieties, superelliptic jacobians, endomorphisms of abelian varieties.

1. Definitions and statements

Throughout this paper $K$ is a field and $\overline{K}$ its algebraic closure. We write $\text{Gal}(K)$ for the absolute Galois group $\text{Gal}(\overline{K}/K) := \text{Aut}(\overline{K}/K)$. If $X$ is an abelian variety of positive dimension over $\overline{K}$ then $\text{End}(X)$ stands for the ring of all $\overline{K}$-endomorphisms and $\text{End}_0(X)$ for the corresponding $\mathbb{Q}$-algebra $\text{End}(X) \otimes \mathbb{Q}$.

We write $1_X$ for the identity endomorphism of $X$. If $X$ is defined over $K$ then we write $\text{End}_K(X)$ for the ring of all $K$-endomorphisms of $X$. We have

$\mathbb{Z} = \mathbb{Z} \cdot 1_X \subset \text{End}_K(X) \subset \text{End}(X)$,

$\mathbb{Q} = \mathbb{Q} \cdot 1_X \subset \text{End}_K(X) \otimes \mathbb{Q} =: \text{End}_K^0(X) \subset \text{End}(X)$,

Let $\mathbb{C}$ be the field of complex numbers, $q$ a positive integer, $\zeta_q \in \mathbb{C}$ a primitive $q$th root of unity, $\mathbb{Q}(\zeta_q) \subset \mathbb{C}$ the $q$th cyclotomic field and $\mathbb{Z}[\zeta_q]$ the ring of integers in $\mathbb{Q}(\zeta_q)$.

1.1. Let $\ell$ be a prime such that $\text{char}(K) \neq \ell$. Let $f(x) \in K[x]$ be a polynomial of degree $n \geq 3$ without multiple roots, $\mathfrak{R}_f \subset K_n$ the $(n$-element) set of roots of $f$ and $K(\mathfrak{R}_f) \subset K_n$ the splitting field of $f$. We write $\text{Gal}(f) = \text{Gal}(f/K)$ for the Galois group $\text{Gal}(K(\mathfrak{R}_f)/K)$ of $f$; it permutes the roots of $f$ and may be viewed as a certain permutation group of $\mathfrak{R}_f$, i.e., as a subgroup of the group $\text{Perm}(\mathfrak{R}_f) \cong S_n$ of all permutations of $\mathfrak{R}_f$. We write $\text{Alt}(\mathfrak{R}_f) \cong A_n$ for the only subgroup of index 2 in $\text{Perm}(\mathfrak{R}_f)$ that consists of all even permutations of $\mathfrak{R}_f$. Slightly abusing notation, we say that $\text{Gal}(f)$ is the full symmetric group $S_n$ (resp. the alternating group $A_n$) if $\text{Gal}(f) = \text{Perm}(\mathfrak{R}_f)$ (resp. $\text{Alt}(\mathfrak{R}_f)$).

Let us consider the standard faithful permutational representation of the group of permutation $\text{Gal}(f) \subset \text{Perm}(\mathfrak{R}_f)$ in the $n$-dimensional $\mathbb{F}_\ell$-vector space

$\mathbb{F}_\ell^{\mathfrak{R}_f} = \{ \phi : \mathfrak{R}_f \to \mathbb{F}_\ell \}$
of \( \mathbb{F}_\ell \)-valued functions on \( \mathfrak{R}_f \) and its \((n-1)\)-dimensional subrepresentation in the subspace

\[
\left( \mathbb{F}_\ell^{\mathfrak{R}_f} \right)^0 := \{ \phi : \mathfrak{R}_f \to \mathbb{F}_\ell \mid \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = 0 \}
\]

(see [4]). The natural surjection

\[
\text{Gal}(K) \to \text{Gal}(K(\mathfrak{R}_f)/K) = \text{Gal}(f)
\]

provides \( \mathbb{F}_\ell^{\mathfrak{R}_f} \) with the natural structure of \( \text{Gal}(K) \)-module and \( \left( \mathbb{F}_\ell^{\mathfrak{R}_f} \right)^0 \) becomes its \( \text{Gal}(K) \)-submodule.

1.2. Let \( C_{f,\ell} \) be a smooth projective model of the smooth affine \( K \)-curve \( y^\ell = f(x) \); its genus \( g \) is equal to \((n-1)(l-1)/2\) if \( \ell \) does not divide \( n \) and to \((n-1)(l-1)/2\) if \( \ell \) divides \( n \). The jacobian \( J(C_{f,\ell}) \) of \( C_{f,\ell} \) is a \( g \)-dimensional abelian variety that is defined over \( K \).

Suppose that \( K \) contains a primitive \( \ell \)-th root of unity say, \( \zeta \). The map \((x, y) \mapsto (x, \zeta y)\) gives rise to a non-trivial birational \( K \)-automorphism \( \delta_\ell : C_{f,\ell} \to C_{f,\ell} \) of period \( \ell \). By Albanese functoriality, \( \delta_\ell \) induces an automorphism of \( J(C_{f,\ell}) \) which we still denote by \( \delta_\ell \). It is known [7, p. 149], [9, p. 458] (see also [24, 26]) that \( \delta_\ell \) satisfies the \( \ell \)-th cyclotomic equation, i.e., \( \delta_\ell^{\ell-1} + \cdots + \delta_\ell + 1 = 0 \) in \( \text{End}(J(C_{f,\ell})) \).

This gives rise to the ring embeddings

\[
\mathbb{Z}[\zeta_\ell] \to \text{End}_K(J(C_{f,\ell})) \subset \text{End}(J(C_{f,\ell})), \quad \zeta_\ell \mapsto \delta_\ell,
\]

\[
\mathbb{Q}[\zeta_\ell] \to \text{End}_K^0(J(C_{f,\ell})) \subset \text{End}^0(J(C_{f,\ell})), \quad \zeta \mapsto \delta_\ell
\]

which send 1 to the identity automorphism of \( J(C_{f,\ell}) \). In particular, if \( \mathbb{Q}[\delta_\ell] \) is the \( \mathbb{Q} \)-subalgebra of \( \text{End}^0(J(C_{f,\ell})) \) generated by \( \delta_\ell \) then the latter embedding establishes a canonical isomorphism of \( \mathbb{Q} \)-algebras

\[
\mathbb{Q}(\zeta_\ell) \cong \mathbb{Q}[\delta_\ell]
\]

that sends \( \zeta_\ell \) to \( \delta_\ell \).

The set of fixed points of \( \delta_\ell \)

\[
J(C_{f,\ell})^{\delta_\ell} := \{ z \in J(C_{f,\ell})(\mathcal{K}_a) \mid \delta_\ell(z) = z \}
\]

is a \( \text{Gal}(K) \)-submodule of \( J(C_{f,\ell})(\mathcal{K}_a) \).

**Lemma 1.3** (See [7, 9]). If \( \ell \) does not divide \( n \) then the the \( \text{Gal}(K) \)-module \( J(C_{f,\ell})^{\delta_\ell} \) is isomorphic to \( \left( \mathbb{F}_\ell^{\mathfrak{R}_f} \right)^0 \) defined by (1).

1.4. Let \( \Omega^1(J(C_{f,\ell})) \) be the \( g \)-dimensional \( \mathcal{K}_a \)-vector space of (invariant) differentials of the first kind on \( J(C_{f,\ell}) \) and

\[
\delta_\ell^* : \Omega^1(J(C_{f,\ell})) \to \Omega^1(J(C_{f,\ell}))
\]

the linear operator induced by functoriality by \( \delta_\ell \). Clearly, \((\delta_\ell^*)^\ell \) is the identity map. Since \( \text{char}(\mathcal{K}_a) \neq \ell \), the linear operator \( \delta_\ell^* \) is diagonalizable. It is known [24, Remarks 4.5, 4.6 and 4.7 on pp. 352–353] that the spectrum of \( \delta_\ell^* \) consists of (primitive) \( \ell \)-th roots of unity \( \zeta^{-i} \) where \( i < \ell \) is a positive integer such that \([ni/\ell] > 0 \) and the multiplicity of \( \zeta^{-i} \) equals \([ni/\ell] \). (In particular, 1 is not an eigenvalue of \( \delta_\ell^* \).)
The structure of the endomorphism algebra of superelliptic jacobians was studied in [20, 22, 19, 24, 26, 27, 28, 14, 15, 29]. In particular, the author proved in [17, 22] that if \( \text{char}(K) = 0 \), then \( \text{Gal}(f) \) is either \( S_n \) or \( A_n \).

The aim of this paper is to extend this results to the case of prime characteristic under an additional assumption that \( J(C,f,\ell) \) is an ordinary abelian variety. Our main result is the following assertion.

**Theorem 1.5.** Suppose that \( K \) is a field of prime characteristic \( p \). Let \( n \geq 5 \) be an integer and \( \ell \) is an odd prime that does not coincide with \( p \). Suppose that \( K \) contains a primitive \( \ell \)-th root of unity say, \( \zeta_\ell \) and \( \text{Gal}(f) \) is either \( S_n \) or \( A_n \). Assume also that \( J(C,f,\ell) \) is an ordinary abelian variety.

If \( (\ell, n) \neq (5, 5) \) then

\[
\text{End}^0(J(C,f,\ell)) = \mathbb{Q}[\delta_\ell] \cong \mathbb{Q}(\zeta_\ell), \quad \text{End}(J(C,f,\ell)) = \mathbb{Z}[\delta_\ell] \cong \mathbb{Z}[\zeta_\ell].
\]

**Corollary 1.6** (Corollary to Theorem 1.5). Suppose that \( K \) is a field of prime characteristic \( p \). Let \( n \geq 5 \) be an integer and \( \ell \) is an odd prime that does not coincide with \( p \). Suppose that \( \text{Gal}(f) = \text{Gal}(f/K) \) coincides either with \( S_n \) or with \( A_n \). Assume also that \( J(C,f,\ell) \) is an ordinary abelian variety.

If \( (\ell, n) \neq (5, 5) \) then

\[
\text{End}(J(C,f,\ell)) \cong \mathbb{Z}[\zeta_\ell], \quad \text{End}^0(J(C,f,\ell)) \cong \mathbb{Q}(\zeta_\ell).
\]

**Proof of Corollary 1.6 (modulo Theorem 1.5).** Let \( \zeta \in K_n \) be a primitive \( \ell \)-th root of unity. Then \( K_1 := K(\zeta) \) is a finite abelian extension of \( K \). Hence the Galois group \( \text{Gal}(f/K_1) \) of \( f(x) \) over \( K_1 \) is the normal subgroup of \( \text{Gal}(f/K) \) and the corresponding quotient is an abelian group. Since \( \text{Gal}(f/K) \) is either \( S_n \) or \( A_n \), and \( n \geq 5 \), the group \( \text{Gal}(f)/K_1 \) is also either \( S_n \) or \( A_n \). Applying Theorem 1.5 to \( (K_1, f(x), \ell) \), we conclude that

\[
\text{End}(J(C,f,\ell)) \cong \mathbb{Z}[\zeta_\ell], \quad \text{End}^0(J(C,f,\ell)) \cong \mathbb{Q}(\zeta_\ell).
\]

\[
\Box
\]

1.7. Now let us assume that \( q = \ell^r \) is a power of a prime \( \ell \neq \text{char}(K) \) and consider the smooth projective model \( C_{f,q} \) of the affine smooth curve \( y^q = f(x) \). If \( K \) contains a primitive \( q \)-th root of unity say, \( \zeta \) then \( C_{f,q} \) admits a periodic \( K \)-automorphism

\[
\delta_q : C_{f,q} \to C_{f,q}, \quad (x, y) \mapsto (x, \zeta y),
\]

which induces by Albanese functoriality the periodic automorphism of \( J(C_{f,q}) \), which we continue denote by

\[
\delta_q \in \text{Aut}_K(J(C_{f,q})).
\]

It is known [24, Lemma 4.8 on p.354] that

\[
\delta_q^\ell = 1_{J(C_{f,q})}, \quad \sum_{i=0}^{\ell-1} \delta_q^{i\ell^{-1}} = 0.
\]

In addition, the \( \mathbb{Q} \)-subalgebra \( \mathbb{Q}[\delta_q] \) of \( \text{End}^0_K(J(C_{f,q})) \) generated by \( \delta_q \) is canonically isomorphic to the direct sum \( \prod_{j=1}^r \mathbb{Q}(\zeta_{\ell^j}) \) of cyclotomic fields (ibid).

The following assertion was proven by the author in [24, Th. 1.1 on p. 340]
Theorem 1.8. Let $K$ be a subfield of $\mathbb{C}$. Suppose that $n \geq 5$ is an integer, $\ell$ is a prime and $r$ a positive integer. Let us assume that either $\ell \nmid n$ or $q := \ell^r$ divides $n$. Suppose that $\text{Gal}(f)$ is either $\mathbf{S}_n$ or $\mathbf{A}_n$. A If $(q,n) \neq (5,5)$ then the semisimple $\mathbb{Q}$-algebra $\text{End}^0(J(C_{f,\ell}))$ coincides with $\mathbb{Q}[\delta_q]$ is isomorphic to the direct sum $\prod_{j=1}^r \mathbb{Q}(\zeta_{\ell^j})$ of cyclotomic fields.

Remark 1.9. J. Xue [14] extended the result of Theorem 1.8 to the remaining case when $\ell \mid n$ but $q$ does not divide $n$.

The second main result of this paper is an analogue of Theorem 1.8 in finite characteristic for ordinary Jacobians.

Theorem 1.10. Suppose that $K$ is a field of prime characteristic $p$. Let $n \geq 5$ be an integer, $\ell$ an odd prime that does not coincide with $p$, $\tau$ a positive integer. Let us assume that either $\ell \nmid n$ or $q := \ell^\tau$ divides $n$. Suppose that $\text{Gal}(f)$ is either $\mathbf{S}_n$ or $\mathbf{A}_n$. Assume also that the Jacobian $J(C_{f,q})$ of $C_{f,q}$ is an ordinary abelian variety.

If $(q,n) \neq (5,5)$ then the semisimple $\mathbb{Q}$-algebra $\text{End}^0(J(C_{f,\ell}))$ coincides with $\mathbb{Q}[\delta_q]$ and is isomorphic to the direct sum $\prod_{j=1}^r \mathbb{Q}(\zeta_{\ell^j})$ of cyclotomic fields.

Remarks 1.11. (ii) Replacing $K$ by its perfectization $\mathbb{F}_p$, we may and will assume in the course of the proof of Theorems 1.5 and 1.10 that $K$ is a perfect field.

(ii) Replacing $K$ by its suitable finite abelian extension, we may and will assume in the course of the proof of Theorems 1.5 and 1.10 that $\text{Gal}(f) = \mathbf{A}_n$ and $K$ contains a primitive $\ell$th root of unity.

(iii) Using an elementary substitution (see [24, Remark 4.3]), we may and will assume in the course of the proof of Theorems 1.5 and 1.10 that $\ell$ does not divide $n$.

Example 1.12. Let us choose positive integers $q \geq 2$ and $d$ and assume that either $q \geq 7$ or $d \geq 2$. Pick an odd prime $p$ that is congruent to 1 modulo $q(dq-1)$. Let us put $n = dq$; clearly, $n \geq 6$. Let $K = \mathbb{F}_p(t)$ be the field of rational functions in one variable over an algebraic closure $\overline{\mathbb{F}}_p$ of the (finite) prime field $\mathbb{F}_p$ of characteristic $p$. Since $p > n$, the product $n(n-1)$ is not divisible by $p$. This implies that the polynomial $f(x) = x^n - x - t \in K[x]$ is a Morse function in a sense of [10, p. 39]; in particular, $\text{Gal}(f) = \mathbf{S}_n$ [10, Th. 4.4.5]. I claim that the Jacobian $J$ of the superelliptic $K$-curve $C : y^q = x^n - x - t$ is an ordinary abelian variety over $K$. In order to prove that, it suffices to check that the Jacobian $J_0$ of its specialization

$$C_0 : y^q = x^n - x = x^{dq} - x$$

(at $t = 0$) is an ordinary abelian variety over $\overline{\mathbb{F}}_p$. Dividing the equation of $C_0$ by $x^n$ and using a substitution

$$u = \frac{y}{x^d}, \quad v = \frac{1}{x},$$

we obtain that $C_0$ is birationally isomorphic to the curve

$$C' : u^q = 1 - v^{dq-1}.$$

Clearly, $C'$ is covered by Fermat curve

$$w^m = 1 - z^m$$

with $m := q(dq-1)$. Since $p-1$ is divisible by $q(dq-1) = m$, the Jacobian of the Fermat curve is ordinary [16, Prop. 4.1 and Th. 4.2]. Since $J_0$ is isomorphic to a
quotient of the jacobian of the Fermat curve, it is also ordinary. This implies that
$J$ is ordinary. Now if $q = ℓ$ is an odd prime then $n = dp ≥ 2ℓ ≥ 6$ and the equality
$\text{End}(J(C, ℓ)) = \mathbb{Z}[\zeta_ℓ]$ follows from Theorem 1.5. (Compare with [25] where the case
of $p = 3, n = 9$ is discussed.)

Similarly, if $r ≥ 2$ is an integer and $q = ℓ^r$ is a power of a prime $ℓ$ then it follows
from Theorem 1.10 that

$\text{End}^0(J(C, ℓ)) \cong \bigoplus_{j=1}^{r} \mathbb{Q}(\zeta_{ℓ^j})$.

Acknowledgements. I am grateful to Noriko Yui and Daqing Wan for stimulating discussions.

2. The plan of the proof

Our proof is based on Serre-Tate canonical lifting of ordinary abelian varieties
[3] and the following assertions.

Theorem 2.1. Suppose that a positive integer $q = ℓ^r$ is a power of a prime $ℓ$
with positive integer $r$, $n ≥ 5$ a positive integer that is not divisible by $ℓ$.
Let $K$ a
field of characteristic zero that contains a primitive $q$th root of unity $ζ_q$.
Let $Y$ be a
positive-dimensional abelian variety over $K$ that admits an endomorphism (actually
an automorphism) $δ_K ∈ \text{End}_K(Y)$ that satisfies the $q$th cyclotomic equation

$$Φ_q(δ_K) = \sum_{i=0}^{ℓ-1} \delta_{r}^{q^{i-1}} = 0$$

in $\text{End}_K(Y)$. Then $δ_K$ and $Y$ enjoy the following properties.

(1) (1i) $δ_K^n = 1_Y$.

(1ii) The ring homomorphism

$$i_{Y} : \mathbb{Z}[ζ_q] → \text{End}_K(Y) ⊂ \text{End}(Y)$$

that sends 1 to $1_Y$ and $ζ_q$ to $δ_K$ is a ring embedding.

(1iii) $φ(q) = |\mathbb{Q}(ζ_q) : \mathbb{Q}|$ divides $2\text{dim}(Y)$.

(2) Assume additionally that $δ_K$ and $Y$ enjoy the following properties.

(2i) Let us consider the $K$-linear map

$$δ_K^* : \Omega^1(Y) → \Omega^1(Y)$$

induced by $δ_K$.

Then all eigenvalues of $δ_K^*$ are primitive $q$th roots of unity. In addition,
for each positive integer $i$ with

$1 ≤ i ≤ q, \ (i, ℓ) = 1$

the multiplicity of $ζ_q^{-i}$ as an eigenvalue of $δ_K^*$ is $[ni/q]$. In particular,
$ζ_q^{-1}$ is an eigenvalue of $δ_K^*$ if and only if $[ni/q] > 0$.

(2ii) The $\text{Gal}(K)$-submodule of fixed points of $δ_K$

$$Y^{δ_K} := \{ y ∈ Y(K) \mid δ_K(y) = y \} ⊂ Y(K)$$

is a $(n - 1)$-dimensional vector space over the prime finite field $\mathbb{F}_ℓ$, the image of $\text{Gal}(K)$ in $\text{Aut}_{\mathbb{F}_ℓ}(Y^{δ_K})$ contains a subgroup isomorphic to
\( \mathbb{A}_n \) and the corresponding \( \mathbb{A}_n \)-module \( \mathcal{Y}^\delta \) is isomorphic to the natural representation of \( \mathbb{A}_n \) in
\[
(\mathbb{F}_\ell^n)^0 := \{ (a_1, \ldots, a_n) \in \mathbb{F}_\ell^n \mid \sum_{i=1}^n a_i = 0 \}.
\]

Then the following conditions hold.

(a) The spectrum of the linear operator \( \delta^*_K \) consists of more that \( \varphi(q) \) distinct eigenvalues.

(b) \[
i_Y (\mathbb{Z}[\zeta_q]) = \text{End}_K(\mathcal{Y}) = \text{End}(\mathcal{Y}),
\]
i.e., \( \text{End}(\mathcal{Y}) \) coincides with its own subring generated by \( \delta_K \) and the ring homomorphism \( i_Y \) is a ring isomorphism. In particular, \( \mathcal{Y} \) is absolutely simple and \( \text{End}^0(\mathcal{Y}) \cong \mathbb{Q}(\zeta_q) \).

**Theorem 2.2.** Suppose that a positive integer \( q = \ell^r \) is a power of a prime \( \ell \) with positive integer \( r \), \( n \geq 5 \) a positive integer that is not divisible by \( \ell \). Let \( K \) a perfect field of prime characteristic \( p \neq \ell \) that contains a primitive \( q \)-th root of unity \( \bar{\zeta} \). Let \( \mathcal{Y} \) be a positive-dimensional abelian variety over \( K \) that admits an endomorphism \( \delta \in \text{End}_K(\mathcal{Y}) \) that satisfies the \( q \)-th cyclotomic equation
\[
(6) \quad \Phi_q(\delta) = \sum_{i=0}^{\ell-1} \delta^{q^{\ell^i-1}} = 0
\]
in \( \text{End}_K(\mathcal{Y}) \). Then \( \delta \) and \( \mathcal{Y} \) enjoy the following properties.

(1) (1i) \( \delta^q = 1_{\mathcal{Y}} \).

(iii) The ring homomorphism
\[
i_Y : \mathbb{Z}[\zeta_q] \to \text{End}_K(\mathcal{Y}) \subset \text{End}(\mathcal{Y})
\]
that sends 1 to \( 1_Y \) and \( \zeta_q \) to \( \delta \) is an embedding.

(iii) \( \varphi(q) = [\mathbb{Q}(\zeta_q) : \mathbb{Q}] \) divides \( 2\dim(\mathcal{Y}) \).

(2) Assume additionally that \( \delta \) and \( \mathcal{Y} \) enjoy the following properties.

(2i) Let us consider the \( K \)-linear map \( \delta^* : \Omega^1(\mathcal{Y}) \to \Omega^1(\mathcal{Y}) \)

induced by \( \delta \).

Then all eigenvalues of \( \delta^* \) are primitive \( q \)-th roots of unity. In addition, for each positive integer \( i \) with
\[
1 \leq i \leq q, \ (i, \ell) = 1
\]
the multiplicity of \( \bar{\zeta}^{-i} \) as an eigenvalue of \( \delta^* \) is \([ni/q]\). In particular, \( \bar{\zeta}^{-i} \) is an eigenvalue of \( \delta^* \) if and only if \([ni/q] > 0 \).

(2ii) The Gal\((K)\)-submodule of fixed points of \( \delta \)
\[
\mathcal{Y}^\delta := \{ y \in Y(\bar{K}) \mid \delta(y) = y \} \subset Y(\bar{K})
\]
is a \((n-1)\)-dimensional vector space over the prime finite field \( \mathbb{F}_\ell \), the image of Gal\(K \in \text{Aut}_{\mathbb{F}_\ell}(\mathcal{Y}^\delta) \) contains a subgroup isomorphic to \( \mathbb{A}_n \) and the corresponding \( \mathbb{A}_n \)-module \( \mathcal{Y}^\delta \) is isomorphic to the natural representation of \( \mathbb{A}_n \) in
\[
(\mathbb{F}_\ell^n)^0 = \{ (a_1, \ldots, a_n) \in \mathbb{F}_\ell^n \mid \sum_{i=1}^n a_i = 0 \}.
\]
Then the following conditions hold.

(a) The spectrum of the linear operator $\delta^*$ consists of more than $\varphi(q)$ distinct eigenvalues.

(b) $i_Y(\mathbb{Z}[\zeta_q]) = \text{End}_K(Y) = \text{End}(Y)$, i.e., $\text{End}(Y)$ coincides with its own subring generated by $\delta$ and the ring homomorphism $i_Y$ is a ring isomorphism. In particular, $Y$ is absolutely simple and $\text{End}^0(Y) \cong \mathbb{Q}(\zeta_q)$

Proof of Theorem 1.5 (modulo Theorem 2.2). In light of Remarks 1.11, we may and will assume that $K$ is a perfect field and $\text{Gal}(f) = \mathbb{A}_n$. and $\ell$ does not divide $n$. Let us put

$$q = \ell, Y = J(C_{f,\ell}), \delta = \delta_{\ell}.$$ 

Let us choose an order on the $n$-element set $\mathcal{R}_f$. This gives us a bijection between $\mathcal{R}_f$ and $\{1, 2, \ldots, n\}$. This gives us the group isomorphism $\text{Gal}(f) \cong \mathbb{A}_n$ and an isomorphism of the corresponding $\mathbb{A}_n$-modules $(\mathbb{F}_q^\ell)^0$ and $(\mathbb{F}_q^n)^0$. Lemma 1.3 and results of Subsection 1.4 imply that all the conditions of Theorem 2.2 are fulfilled. Now the desired result follows from Theorem 2.2. $\square$

3. Endomorphism algebras of abelian varieties

Let $X$ be an abelian variety of positive dimension over an arbitrary field $K$. If $n$ is a positive integer that is not divisible by $\text{char}(K)$ then $X[n]$ stands for the kernel of multiplication by $n$ in $X(K_a)$. It is well-known [5] that $X[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(X)$. In particular, if $n = \ell$ is a prime then $X[\ell]$ is a $2\dim(X)$-dimensional $\mathbb{F}_\ell$-vector space.

If $X$ is defined over $K$ then $X[n]$ is a Galois submodule in $X(K_a)$ and all points of $X[n]$ are defined over a finite separable extension of $K$. We write $\rho_{n,X,K} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X[n])$ for the corresponding homomorphism defining the structure of the Galois module on $X[n]$,

$$\tilde{G}_{n,X,K} \subset \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X[n])$$

for its image $\tilde{\rho}_{n,X,K}(\text{Gal}(K))$ and $K(X[n])$ for the field of definition of all points of $X[n]$. Clearly, $K(X[n])$ is a finite Galois extension of $K$ with Galois group $\text{Gal}(K(X[n])/K) = \tilde{G}_{n,X,K}$. If $n = \ell$ then we get a natural faithful linear representation

$$\tilde{G}_{\ell,X,K} \subset \text{Aut}_{\mathbb{F}_\ell}(X[\ell])$$

of $\tilde{G}_{\ell,X,K}$ in the $\mathbb{F}_\ell$-vector space $X[\ell]$.

Since $X$ is defined over $K$, one may associate with every $u \in \text{End}(X)$ and $\sigma \in \text{Gal}(K)$ an endomorphism $\sigma u \in \text{End}(X)$ such that $\sigma u(x) = \sigma u(\sigma^{-1} x)$ for $x \in X(K_a)$ and we get the group homomorphism

$$\kappa_X : \text{Gal}(K) \to \text{Aut}(\text{End}(X)); \quad \kappa_X(\sigma)(u) = \sigma u \quad \forall \sigma \in \text{Gal}(K), u \in \text{End}(X).$$

It is well-known that $\text{End}_K(X)$ coincides with the subring of $\text{Gal}(K)$-invariants in $\text{End}(X)$, i.e., $\text{End}_K(X) = \{ u \in \text{End}(X) \mid \sigma u = u \quad \forall \sigma \in \text{Gal}(K) \}$. It is also well-known that $\text{End}(X)$ (viewed as a group with respect to addition) is a free commutative group of finite rank and $\text{End}_K(X)$ is its pure subgroup, i.e., the quotient $\text{End}(X)/\text{End}_K(X)$ is also a free commutative group of finite rank.
4. ABELIAN SCHEMES

Let $K$ be a complete discrete valuation field with discrete valuation ring $O_K$ with maximal ideal $m$ and perfect residue field $\kappa := O_K/m$. We write

$$O_K \to O_K/m = \kappa, \ a \mapsto \bar{a} = a + m$$

for the residue map. If $q$ is a positive integer that is not divisible by char($\kappa$) and such that $\kappa$ contains a primitive $q$th root of unity then it follows from Hensel’s Lemma that $O_K$ contains a primitive $q$th root of unity and the reduction map defines a canonical isomorphism

$$\mu_{q,K} \cong \mu_{q,\kappa}, \ \gamma \mapsto \bar{\gamma}$$

between the order $q$ cyclic groups of $q$th roots of unity

$$\mu_{q,K} \subset O_K \subset K^*$$

and $\mu_{q,\kappa} \subset \kappa^*$. Since $K$ is complete, the absolute Galois group $\text{Gal}(K) = \text{Aut}(\bar{K}/K)$ coincides with the decomposition group and the inertia subgroup $I$ of $\text{Gal}(K)$ is a closed normal subgroup of $\text{Gal}(K)$. The natural extension of the reduction map to $\bar{K}$ induces the surjective continuous group homomorphism [12, Sect. 1]

$$\text{red}_n : \text{Gal}(K)/I \to \text{Gal}(\kappa),$$

which is actually an isomorphism of compact (profinite) groups.

We write $S$ for Spec($O_K$). It is well known that $S$ consists of generic point $\eta$ that corresponds to $\{0\}$ and closed point $s$ that corresponds to $m$.

Let $f : X \to S$ be an abelian scheme over $S$ of positive relative dimension $g$. We write $X_K$ for its generic fiber, which is a $g$-dimensional abelian variety over $K$, and $X_s$ for its closed fiber, which is a $g$-dimensional abelian variety over $\kappa$. By definition, $X$ is a separated scheme; it is known [2, Remark 1.2 on p. 1] that $X$ is a scheme of finite type over $S$ and therefore is noetherian. In addition, $X$ is a Néron model of $X_K$ [1, Prop. 8 on p. 15]. In particular, the natural ring homomorphism

$$\text{End}_S(X) \to \text{End}(X_K), \ u \mapsto u_K$$

is an isomorphism. Notice that the natural ring homomorphism

$$\text{End}_S(X) \to \text{End}(X_s), \ u \mapsto u_s$$

is an embedding.

As usual, we write $O_X$ for the structure sheaf of $X$. Clearly, the ring $\Gamma(X, O_X)$ of global sections of $X$ is a $O_K$-algebra. Since $f$ is proper, the $O_K$-module $\Gamma(X, O_X)$ is finitely generated.

The following assertion is contained in [12, Theorem 1 on p. 493 and Lemma 2 on p. 495].

**Lemma 4.1.** Let $n$ be a positive integer that is not divisible by char($\kappa$).

(i) The action of the inertia subgroup $I$ on the $\text{Gal}(K)$-module $X_K[n]$ is trivial and therefore one may view $X_K[n]$ as the $\text{Gal}(\kappa)$-module via (8).

(ii) There is a canonical isomorphism of $\text{Gal}(\kappa)$-modules

$$\text{red}_n : X_K[n] \cong X_s[n]$$
such that the diagram

\[
\begin{array}{ccc}
X_K[n] & \xrightarrow{\text{red}_n} & X_K[n] \\
\downarrow & \text{red}_n & \downarrow \\
X_s[n] & \xrightarrow{u_s} & X_s[n]
\end{array}
\]

is commutative for all \(u \in \text{End}_S(\mathcal{X})\).

- The \(\text{Gal}(\kappa)\)-modules of fixed points

\[
X_K[n]^{\text{uk}} = \{x \in X_K[n] \mid u_K(x) = x\}
\]

and

\[
X_s[n]^{u_s} = \{x \in X_s[n] \mid u_s(x) = x\}
\]

are isomorphic for all \(u \in \text{End}_S(\mathcal{X})\).

\textbf{Proof.} (i) follows from [12, Theorem 1 on p. 493 and Lemma 2 on p. 495]. This implies that \(X_K[n]^f = X_K[n]\).

The desired isomorphism of Galois modules

\[
\text{red}_n = X_K[n]^f = X_K[n] \cong X_s[n]
\]

is constructed in the proof of Lemma 2 on p. 495 of [12]. It follows readily from the construction that all the diagrams (12) are commutative. This proves (ii), which immediately implies (iii). \(\square\)

The following assertion is certainly well known but I failed to find a suitable reference.

\textbf{Lemma 4.2.} The scheme \(\mathcal{X}\) is normal reduced irreducible and \(\Gamma(X, \mathcal{O}_X) = O_K\).

\textbf{Proof.} The abelian scheme \(\mathcal{X}\) is automathically of finite presentation over \(S\) [2, Remark 1.2(a) on p. 3]. Since \(S\) is normal and \(f : \mathcal{X} \to S\) is smooth, it follows from [6, Prop. 5.5 on pp. 235–236] that \(\mathcal{X}\) is normal and therefore reduced. It follows from [6, Criterion 5.5.2 on pp. 234–235] that the irreducible components of the topological space \(\mathcal{X}\) are disjoint. Since \(X_K\) is a nonempty open irreducible subset of \(\mathcal{X}\), it lies in an irreducible component of \(\mathcal{X}\) say, \(Y_1\). Since \(X_s\) is a nonempty closed irreducible subset of \(\mathcal{X}\), it lies in an irreducible component of \(\mathcal{X}\) say, \(Y_2\). This implies that the topological space \(\mathcal{X}\) is a union of \(Y_1\) and \(Y_2\). Since irreducible components are closed subsets, both \(Y_1\) and \(Y_2\) are closed subsets in \(\mathcal{X}\). Since \(f\) is proper, \(f(Y_1)\) is a closed subset of \(S\). By definition, \(f(Y_1)\) contains the generic point \(\eta\) of \(S\) and therefore contains its closure \(S\). This implies that \(f(Y_1) = S\). Hence \(Y_1\) meets \(X_s\) and therefore meets \(Y_2\) as well. It follows that \(Y_1 = Y_2\) and therefore \(\mathcal{X} = Y_1\) is irreducible. This implies that \(\Gamma(X, \mathcal{O}_X)\) is an \(O_K\)-algebra without zero divisors. On the other hand, the properness of \(f\) implies that the \(O_K\)-algebra \(\Gamma(X, \mathcal{O}_X)\) is a finitely generated \(\Gamma(S, \mathcal{O}_S) = O_K\)-module.

Recall that \(X_K\) is an open nonempty subset of \(\mathcal{X}\). The irreducibility of \(\mathcal{X}\) implies that \(X_K\) is dense in \(\mathcal{X}\). It follows that the restriction map

\[
\Gamma(X, \mathcal{O}_X) \to \Gamma(X_K, \mathcal{O}_{X_K}) = K
\]

is injective. This implies that the (isomorphic) image of \(\Gamma(X, \mathcal{O}_X)\) in \(K\) is an order containing \(O_K\) and therefore coincides with \(O_K\). It follows that \(\Gamma(X, \mathcal{O}_X) = O_K\). \(\square\)
We write $\Omega^1(X_K)$ and $\Omega^1(X_s)$ for the $K$-vector space $\Omega^1(X_K)$ of differentials of the first kind on $X_K$ and the $\kappa$-vector space $\Omega^1(X_s)$ of differentials of the first kind on $X_s$ respectively (both of dimension $g$).

**Theorem 4.3.** Let $q$ be a positive integer that is not divisible by $\text{char}(\kappa)$ such that $\kappa$ contains a primitive $qth$ root of unity.

Suppose that $\delta_S$ is an automorphism of the abelian scheme $\mathcal{X}/S$ such that $\delta^N_S$ is the identity map. Let $\delta_K : X_K \to X_K$ and $\delta_s : X_s \to X_s$ be the automorphisms of abelian varieties $X_K$ and $X_s$ induced by $\delta_S$. Let us consider the linear automorphisms

$$\delta_K^* : \Omega^1(X_K) \to \Omega^1(X_K), \quad \delta_s^* : \Omega^1(X_s) \to \Omega^1(X_s)$$

induced by $\delta_K$ and $\delta_s$ respectively.

Let $\text{spec}(\delta_K^*) \subset \bar{K}$ and $\text{spec}(\delta_s^*) \subset \bar{\kappa}$ be the sets of eigenvalues of $\delta_K^*$ and $\delta_s^*$ respectively.

Then:

(i) Both $\delta_K^*$ and $\delta_s^*$ are diagonalizable linear operators and

$$\text{spec}(\delta_K^*) \subset \mu_{q,K}, \quad \text{spec}(\delta_s^*) \subset \mu_{q,\kappa}.$$ 

(ii) A root of unity $\gamma \in \mu_q$ lies in $\text{spec}(\delta_s^*)$ if and only if $\bar{\gamma}$ lies in $\text{spec}(\delta_K^*)$.

(iii) The multiplicity of each $\gamma \in \text{spec}(\delta_K^*)$ coincides with the multiplicity of $\bar{\gamma} \in \text{spec}(\delta_s^*)$.

**Proof.** Clearly,

$$\left(\delta_K^*\right)^q = 1_{X_K}, \quad \left(\delta_s^*\right)^N = 1_{X_s}$$

and therefore both $(\delta_K^*)^N$ and $(\delta_s^*)^N$ are the identity automorphisms of $\Omega^1(X_K)$ and $\Omega^1(X_s)$ respectively. The conditions on $q$ imply that both $\delta_K^*$ and $\delta_s^*$ are diagonalizable and their eigenvalues lie in $\mu_{q,K}$ and $\mu_{q,\kappa}$ respectively. This proves (i).

In order to prove (ii) and (iii), recall [1, Cor. 3 on p. 102] that the sheaf $\Omega^1_{\mathcal{X}/S}$ of relative differentials is a free $\mathcal{O}_X$-module of rank $g$ and therefore is generated by certain $g$ sections that remain linearly independent at every point of $\mathcal{X}$. It follows from Lemma 4.2 that the group $\Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}/S})$ of its global sections is a free $\mathcal{O}_K$-module of rank $g$. Let

$$\delta_S^* : \Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}/S}) \to \Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}/S})$$

is the automorphism of $\Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}/S})$ induced by $\delta$. Clearly, $(\delta_S^*)^N$ is the identity map. Our conditions on $N$ imply the existence of a basis $\{\omega_1, \ldots, \omega_g\}$ of $\Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}/S})$ such that for each $i = 1, \ldots, g$ there exists $\gamma_i \in \mu_{N,K}$ such that

$$\delta_S^* \omega_i = \gamma_i \omega_i.$$ 

Clearly, $\{\omega_1, \ldots, \omega_g\}$ remain linearly independent at every point of $\mathcal{X}$. This implies that their restrictions $\{\omega_{1,s}, \ldots, \omega_{g,s}\}$ to $X_s$ constitute a basis of $\kappa$-vector space

$$\Gamma(X_s, \Omega^1_{X_s/\kappa}) = \Omega^1(X_s),$$

their restrictions $\{\omega_{1,K}, \ldots, \omega_{g,K}\}$ to $X_K$ constitute a basis of $K$-vector space

$$\Gamma(X_K, \Omega^1_{X_K/K}) = \Omega^1(X_K).$$
The functoriality of the formation of relative differentials and its compatibility with
base change [1, Prop. 3 on p. 34 and p. 35] imply that
\[ \delta^*_K \omega_{i,K} = \gamma_i \cdot \omega_{i,K}, \quad \delta^*_s \omega_{i,s} = \gamma_i \cdot \omega_{i,s}. \]
for all \( i = 1, \ldots, g \). This implies readily (ii) and (iii).

\[ \square \]

**Theorem 4.4.** We keep the notation and assumptions of Theorem 4.3. Suppose
that there exist a prime \( \ell \) and a positive integer \( r \) such that \( q = \ell^r \) (in particular, \( \ell \neq \text{char}(\kappa) \), the field \( \kappa \) contains a primitive \( \ell^r \)th root of unity) and \( \delta_S \in \text{End}_S(X) \)
satisfies the qth cyclotomic equation
\[ \Phi_{\ell^r}(\delta) = 0 \]
where
\[ \Phi_{\ell^r}(t) = \frac{t^{\ell^r} - 1}{t^{\ell^r - 1} - 1} = \sum_{j=0}^{t-1} t^{j \ell^r - 1} \in \mathbb{Z}[t]. \]

Let us consider the subgroups of fixed points
\[ X_{\delta_K} = \{ x \in X_K(\overline{K}) \mid \delta_K(x) = x \} \subset X_K(\overline{K}) \]
and
\[ X_{\delta_s} = \{ y \in X_s(\mathbb{K}) \mid \delta_s(y) = y \} \subset X_s(\mathbb{k}). \]
Then:
(i) \( X_{\delta_K} \) is a \( \text{Gal}(K) \)-submodule of \( X_K[\ell] \) and \( X_{\delta_s} \) is a \( \text{Gal}(\kappa) \)-submodule of \( X_s[\ell] \).
(ii) \( X_{\delta_K} \) viewed as the \( \text{Gal}(K) \)-module is isomorphic to \( X_{\delta_K} \).

**Proof.** (i) Obvious.
(ii) It follows readily from Lemma 4.1 applied to \( n = \ell \) and \( u = \delta \). \[ \square \]

5. **Canonical liftings**

Let \( \kappa \) be a perfect field of prime characteristic \( p \), \( W(\kappa) \) its ring of Witt vectors
and \( \mathbb{K} \) the field of fractions of \( W(\kappa) \). The field \( \mathbb{K} \) is a complete discrete valuation
field of characteristic zero with valuation ring \( W(\kappa) \) and residue field \( \kappa \).

Let \( X_0 \) be an abelian variety over \( \kappa \) of positive dimension \( g \). If \( X_0 \) is ordinary
then there exists a canonical Serre-Tate lifting of \( X \) - an abelian scheme \( X \) over
\( S = \text{Spec}(W(\kappa)) \), whose closed fiber coincides with \( X \), and the natural ring ho-
momorphism \( \text{End}_S(X) \to \text{End}_S(X_0) \) is an isomorphism [3, p. 172, Th. 3.3]. We
write \( X_K \) for the generic fiber of \( X \); it is a \( g \)-dimensional abelian variety over \( \mathbb{K} \).
The abelian scheme \( X \) is a Néron model of \( X_K \) and therefore the natural ring
homo-morphism \( \text{End}_S(X) \to \text{End}_K(X_K) \) is an isomorphism [1].

6. **Abelian varieties with multiplications**

Let \( E \) be a number field. Let \((X, i)\) be a pair consisting of an abelian variety \( X \)
of positive dimension over \( K_a \) and an embedding \( i : E \hookrightarrow \text{End}^0(X) \). Here \( 1 \in E \)
must go to \( 1_X \).

**Remark 6.1.** It is well known [13, Prop. 2 on p. 36]) that the degree \([E : \mathbb{Q}]\)
divides \( 2 \dim(X) \), i.e.
\[ d_{X,E} := \frac{2 \dim(X)}{[E : \mathbb{Q}]} \]
is a positive integer.

Let us denote by \( \text{End}^0(X, i) \) the centralizer of \( i(E) \) in \( \text{End}^0(X) \). Clearly, \( i(E) \) lies in the center of the finite-dimensional \( \mathbb{Q} \)-algebra \( \text{End}^0(X, i) \). It follows that \( \text{End}^0(X, i) \) carries a natural structure of finite-dimensional \( E \)-algebra.

Let \( \mathcal{O} \) be the ring of integers in \( E \). If \( \mathfrak{a} \) is a non-zero ideal in \( \mathcal{O} \) then the quotient \( \mathcal{O}/\mathfrak{a} \) is a finite commutative ring. Let \( \lambda \) be a maximal ideal in \( \mathcal{O} \). We write \( k(\lambda) \) for the corresponding (finite) residue field \( \mathcal{O}/\lambda \) and \( \ell \) for \( \text{char}(k(\lambda)) \). We have \( \mathcal{O} \supset \lambda \supset \ell \cdot \mathcal{O} \).

Remark 6.2. (See [27, Remark 3.3].) Let us assume that \( \lambda \) is the only maximal ideal of \( \mathcal{O} \) dividing \( \ell \), i.e., \( \ell \cdot \mathcal{O} = \lambda^b \) where the positive integer \( b \) satisfies \( [E: \mathbb{Q}] = b \cdot [k(\lambda): \mathbb{F}_\ell] \).

(i) We have \( \mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_\lambda \) where \( \mathcal{O}_\lambda \) is the completion of \( \mathcal{O} \) with respect to \( \lambda \)-adic topology. It The ring \( \mathcal{O}_\lambda \) is a local principal ideal domain, its only maximal ideal is \( \lambda \mathcal{O}_\lambda \) and
\[
\ell \cdot \mathcal{O}_\lambda = (\lambda \mathcal{O}_\lambda)^b.
\]
(ii) Let us choose an element \( c \in \lambda \) that does not lie in \( \lambda^2 \). Then
\[
\lambda^j = \ell \cdot \mathcal{O} + c^j \cdot \mathcal{O},
\]
This implies that for all positive integers \( j \leq b \)
\[
\lambda^j = \ell \cdot \mathcal{O} + c^j \cdot \mathcal{O}.
\]
In particular,
\[
\ell \cdot \mathcal{O}_\lambda = c^b \cdot \mathcal{O}_\lambda.
\]
It follows that
\[
c^{-j} \ell \cdot \mathcal{O}_\lambda = c^{-j} \cdot \mathcal{O}_\lambda.
\]
(iii) Notice that \( E_\lambda = E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathcal{O} \otimes_{\mathcal{O}_\lambda} \mathcal{O}_\lambda \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \) is the field coinciding with the completion of \( E \) with respect to \( \lambda \)-adic topology.

Suppose that \( X \) is defined over \( K \) and \( i(\mathcal{O}) \subset \text{End}_K(X) \). Then we may view elements of \( \mathcal{O} \) as \( K \)-endomorphisms of \( X \). We write \( \text{End}(X, i) \) for the centralizer of \( i(\mathcal{O}) \) in \( \text{End}(X) \) and \( \text{End}_K(X, i) \) for the centralizer of \( i(\mathcal{O}) \) in \( \text{End}_K(X) \). Obviously, \( \text{End}(X, i) \) is a pure subgroup in \( \text{End}(X) \) and \( \text{End}_K(X, i) = \text{End}(X, i) \cap \text{End}_K(X) \) is a pure subgroup in \( \text{End}(X, i) \), i.e. the quotients \( \text{End}(X)/\text{End}(X, i) \) and \( \text{End}(X, i)/\text{End}_K(X, i) \) are torsion-free. We have
\[
i(\mathcal{O}) \subset \text{End}_K(X, i) \subset \text{End}(X, i) \subset \text{End}(X).
\]
It is also clear that
\[
\text{End}(X, i) = \text{End}^0(X, i) \cap \text{End}(X),
\]
\[
\text{End}^0(X, i) = \text{End}(X, i) \otimes \mathbb{Q} \subset \text{End}(X) \otimes \mathbb{Q} = \text{End}^0(X).
\]
Clearly, \( \text{End}(X, i) \) carries a natural structure of finitely generated torsion-free \( \mathcal{O} \)-module. Since \( \mathcal{O} \) is a Dedekind ring, it follows that there exist non-zero ideals \( b_1, \ldots, b_t \) in \( \mathcal{O} \) such that
\[
\mathbb{Z} \cdot 1_X \subset \text{End}(X, i) \cong b_1 \oplus \cdots \oplus b_t.
\]
Clear, \(\kappa(\sigma)(\text{End}(X, i)) = \text{End}(X, i)\) for all \(\sigma \in \text{Gal}(K)\) and

\[
\text{End}_K(X, i) = \{u \in \text{End}(X, i) \mid \sigma u = u \ \forall \sigma \in \text{Gal}(K)\}.
\]

Let us assume that \(\text{char}(K)\) does not divide the order of \(O/a\) and put

\[
X[a] := \{x \in X(K) \mid i(e)x = 0 \ \forall e \in a\}.
\]

For example, assume that \(\ell \neq \text{char}(K)\). Then the order of \(O/\lambda = k(\lambda)\) is a power of \(\ell\) and \(X[\lambda] \subset X[\ell]\).

Clearly, \(X[a]\) is a Galois submodule of \(X(K)\). It is also clear that \(X[a]\) carries a natural structure of \(O/a\)-module. (It is known [11, Prop. 7.20] that this module is free.)

**Remark 6.3.** Assume in addition that \(\lambda\) is the only maximal ideal of \(O\) dividing \(\ell\) and pick \(c \in \lambda \setminus \lambda^2 \subset \lambda \subset O\).

By Remark 6.2(ii), \(\lambda\) is generated by \(\ell\) and \(c\). Therefore

\[
X[\lambda] = \{x \in X[\ell] \mid cx = 0\} \subset X[\ell].
\]

More generally, for all positive integers \(j \leq b\) the ideal \(\lambda^j\) is generated by \(\ell\) and \(c_j\), which implies that

\[
X[\lambda^j] = \{x \in X[\ell] \mid c^j x = 0\} \subset X[\ell].
\]

Obviously, every endomorphism from \(\text{End}(X, i)\) leaves invariant the subgroup \(X[\lambda] \subset X(K)\) and induces an endomorphism of the \(O/a\)-module \(X[a]\). This gives rise to a natural homomorphism

\[
\text{End}(X, i) \to \text{End}_{O/a}(X[a]),
\]

whose kernel contains \(a \cdot \text{End}(X, i)\). Actually, the kernel coincides with \(a \cdot \text{End}(X, i)\), i.e., there is an embedding

\[
\text{End}(X, i) \otimes_O k(\lambda) \hookrightarrow \text{End}_{O/a}(X[a]).
\]

See [27, pp. 699-700] for the proof.

Now we concentrate on the case of \(a = \lambda\), assuming that \(\ell \neq \text{char}(K)\).

Then \(X[\lambda]\) carries the natural structure of a \(k(\lambda)\)-vector space provided with the structure of Galois module and (15) gives us the embedding

\[
\text{End}(X, i) \otimes_O k(\lambda) \hookrightarrow \text{End}_{k(\lambda)}(X[\lambda]).
\]

Further we will identify \(\text{End}(X, i) \otimes_O k(\lambda)\) with its image in \(\text{End}_{k(\lambda)}(X[\lambda])\). We write

\[
\tilde{\rho}_{\lambda,X} : \text{Gal}(K) \to \text{Aut}_{k(\lambda)}(X[\lambda])
\]

for the corresponding (continuous) homomorphism defining the Galois action on \(X[\lambda]\). It is known [11, Prop. 7.20] (see also [8]) that

\[
\dim_{k(\lambda)} X[\lambda] = \frac{2\dim(X)}{[E : \mathbb{Q}]} := d_{X,E}.
\]

Let us put

\[
\tilde{G}_{\lambda,X} = \tilde{G}_{\lambda,i,X} := \tilde{\rho}_{\lambda,X}(\text{Gal}(K)) \subset \text{Aut}_{k(\lambda)}(X[\lambda]).
\]
Clearly, $\tilde{G}_{\lambda,X}$ coincides with the Galois group of the field extension $K(X[\lambda])/K$ where $K(X[\lambda])$ is the field of definition of all points in $X[\lambda]$.

It is also clear that the image of $\text{End}_{K}(X,i) \otimes_{O} k(\lambda)$ lies in the centralizer $\text{End}_{\tilde{G}_{\lambda,i,X}}$ of $\tilde{G}_{\lambda,i,X}$ in $\text{End}_{k(\lambda)}(X[\lambda])$.

**Lemma 6.4.** (See [27, Lemma 3.8].) Suppose that $i(O) \subset \text{End}_{K}(X)$. If $\lambda$ is a maximal ideal in $O$ such that $\ell \neq \text{char}(K)$ and $\text{End}_{\tilde{G}_{\lambda,X,K}}(X[\lambda]) = k(\lambda)$ then $\text{End}_{K}(X,i) = O$.

7. **Proof of Theorem 2.1**

The ring homomorphism $i_{Y}$ defined in (5) is an embedding, because the $q$th cyclotomic polynomial is irreducible over $\mathbb{Q}$. This proves the first assertion of Theorem 2.1.

The assertion about the cardinality of the spectrum of $\delta_{K}$ is actually proven on pp. 357–358 of [24].

Let us put $E = \mathbb{Q}(\zeta_{q}), O = \mathbb{Z}[\zeta_{q}] \subset \mathbb{Q}(\zeta_{q}) = E$ and write $\lambda$ for the maximal ideal $(1 - \zeta_{q})O$ of $O$. It is well known that $\lambda$ is the only maximal ideal of $O$ that lies above $\ell$ and the field

$$k(\lambda) = O/\lambda = \mathbb{F}_{\ell}.$$ 

Recall [24] that $Y_{\lambda} = \{ y \in Y(K) \mid i_{Y}(e)y = 0 \ \forall e \in O \}$. Clearly,

$$Y_{\lambda} = \{ y \in Y(K) \mid (1_{Y} - \delta_{K})y = 0 \} = \mathbb{Y}^{i}.$$ 

Combining Condition (2ii) of Theorem 2.1 and (16), we obtain that

$$n - 1 = \frac{2\dim(\mathbb{Y})}{[E : \mathbb{Q}]}, \quad 2\dim(\mathbb{Y}) = (n - 1)\varphi(q).$$

Let $\mathbb{Q}[\delta_{K}]$ be the $\mathbb{Q}$-subalgebra of $\text{End}^{0}(\mathbb{Y})$ generated by $\delta_{K}$. Actually, $\mathbb{Q}[\delta_{K}]$ is a (sub)field isomorphic to $\mathbb{Q}(\zeta_{q})$. We write $\text{End}^{0}(\mathbb{Y},i_{Y})$ for the centralizer of $\mathbb{Q}[\delta_{K}]$ in $\text{End}^{0}(\mathbb{Y})$. Clearly

$$\delta_{K} \in \mathbb{Q}[\delta_{K}] \subset \text{End}^{0}(\mathbb{Y},i_{Y}) \subset \text{End}^{0}(\mathbb{Y}).$$

It follows from condition (ii) and Theorem 4.7 of [20] that the $\text{Gal}(K)$-module $\mathbb{Y}_{\lambda}$ is very simple in a sense of [18]. It follows from Theorem 3.8 of [24] that one of the following conditions holds.

(a) The subring $i_{Y}(O)$ coincides with its own centralizer in $\text{End}(Y)$. In other words, every endomorphism in $\text{End}(\mathbb{Y})$ that commutes with $\delta_{K}$ may be presented as a polynomial in $\delta_{K}$ with integer coefficients. Equivalently, $\mathbb{Q}[\delta_{K}] = \text{End}^{0}(\mathbb{Y},i_{Y})$.

(b) $\text{End}^{0}(\mathbb{Y},i_{Y})$ of $\mathbb{Q}[\delta]$ is a central simple $\mathbb{Q}[\delta_{K}]$-algebra of dimension $(2\dim(\mathbb{Y})/[E : \mathbb{Q}])^{2}$. (It follows from (17) that the $\mathbb{Q}[\delta_{K}]$-dimension of $\text{End}^{0}(\mathbb{Y},i_{Y})$ is $(n - 1)^{2}$.)
Let us prove that the case (b) does not occur. Every eigenspace of $\delta^*$ is invariant under the natural action of $\text{End}^0(\mathcal{Y})$. The properties of $\text{End}^0(\mathcal{Y})$ imply that the multiplicity of every eigenvalue of $\delta^*_K$ is divisible by $(n - 1)$. (It is the only place where we use that $\text{char}(K) = 0$.) Notice that for each positive integer $i < q$ with $(i, \ell) = 1$

\[(18) \quad \left[\frac{ni}{q}\right] + \left[\frac{n(q - i)}{q}\right] = n - 1.\]

This implies that if $\zeta^{-i}$ is an eigenvalue of $\delta^*_K$ then its multiplicity $[ni/q]$ is a positive integer divisible by $(n - 1)$ and therefore equals $(n - 1)$. By (18), $[n(q - i)/q] = 0$, i.e., $\zeta^{-(q-i)} = \zeta^{-i}$ is not an eigenvalue of $\delta^*_K$. This implies that the number of distinct eigenvalues of $\delta^*$ does not exceed $\varphi(q)/2$, which is not true. This proves that the case (b) does not occur.

So, the case (a) holds, i.e., the field $\mathbb{Q}[\delta_K] \cong \mathbb{Q}(\zeta_q)$ coincides with its own centralizer in $\text{End}^0(\mathcal{Y})$. Then $\mathbb{Q}[\delta_Y]$ contains the center $\mathcal{C}_Y$ of $\text{End}^0(\mathcal{Y})$. It follows from Corollary 2.2 of [24] that $\mathbb{Q}[\delta_Y]$ coincides with $\mathcal{C}_Y$. This implies that the centralizer of $\mathbb{Q}[\delta_K]$ is the whole $\text{End}^0(\mathcal{Y})$ and therefore $\text{End}^0(\mathcal{Y}) = \mathbb{Q}[\delta_K]$. Since $\mathbb{Z}[\delta_K] \cong \mathbb{Z}[\zeta_q]$ and $\mathbb{Z}[\zeta_q]$ is the maximal order in $\mathbb{Q}[\zeta_q]$, $\text{End}(\mathcal{Y}) = \mathbb{Z}[\delta_K] \cong \mathbb{Z}[\zeta_q]$.

This ends the proof of Theorem 2.1.

8. Proof of Theorem 2.2

Let $W(K)$ be the ring of Witt vectors over $K$ and $\mathbf{K}$ its field of fractions, which has characteristic 0. Since $K$ contains a primitive $q$th root of unity, there is a primitive $q$th root of unity

$$
\zeta \in W(K) \subset \mathbf{K},
$$

that goes to $\zeta$ in $K$ under the reduction map.

Let $S := \text{Spec}(W(K))$ and $f : \mathcal{Y} \to S$ be the canonical Serre-Tate lifting of $Y$ [3], which is an abelian scheme over $S$, whose closed fiber is $Y$. We write $Y$ for the generic fiber of $f$, which is an abelian variety over $\mathbf{K}$ with the same dimension as $Y$. We know (see Section 5) that the natural ring isomorphisms

\[\text{End}_K(\mathcal{Y}) \leftarrow \text{End}_S(\mathcal{Y}) \to \text{End}_{\mathbf{K}}(\mathcal{Y})\]

are isomorphisms. Let $\delta_S \in \text{End}_S(\mathcal{Y})$ be the preimage (lifting) of $\delta$ in $\text{End}_S(\mathcal{Y})$ and $\delta_K \in \text{End}_K(\mathcal{Y})$ be the image (restriction to the generic fiber) of $\delta_S$ in $\text{End}_K(\mathcal{Y})$. Isomorphisms (19) induce ring isomorphisms

\[(20) \quad \mathbb{Z}[\delta_K] \leftarrow \mathbb{Z}[\delta_S] \to \mathbb{Z}[\delta].\]

In light of (2.2),

\[(21) \quad \Phi_\mathcal{Y}(\delta_S) = 0, \quad \Phi_\mathcal{Y}(\delta_K) = 0; \quad \delta_S^\mathcal{Y} = 1_{\mathcal{Y}}, \quad \delta_K^\mathcal{Y} = 1_{\mathcal{Y}}.\]

Then the ring homomorphism

\[i_\mathcal{Y} : \mathbb{Z}[\zeta_q] \to \mathbb{Z}[\delta_K] \subset \text{End}_K(\mathcal{Y})\]

that sends 1 to $1_{\mathcal{Y}}$ and $\zeta_q$ to $\delta_K$ is a ring embedding. This proves Theorem 2.2(1).

In order to prove Theorem 2.2(2), we are going to apply Theorem 2.1 to $\mathcal{Y}/K$. 


Theorems 4.4 and 4.3 applied to \( \mathcal{V}/S \) imply that all the conditions of Theorem 2.1 are fulfilled. Applying Theorem 2.1(2) to \( \mathcal{V}/K, \delta_K, \zeta \), we conclude that

\[
i_Y(\mathbb{Z}[\zeta_q]) = \text{End}_K(\mathcal{V}) = \text{End}(\mathcal{V}).
\]

It remains to recall that there is a canonical ring isomorphism between \( \text{End}(Y) \) and \( \text{End}(\mathcal{V}) \) under which \( \delta = i_Y(\zeta_q) \) goes to \( \delta_K = i_K(\delta_K) \).

9. SUPERELLIPTIC JACOBIANS

We are heading for the proof of Theorem 1.10. We keep the notation of Section 1. In particular, \( \ell \) is a prime, \( K \) is a field of characteristic \( p \neq \ell \) that contains \( \zeta \), which is a primitive \( q = \ell^r \)th root of unity; \( f(x) \in K[x] \) is a polynomial of degree \( n \geq 4 \) and without multiple roots.

We write \( C_{f,q} \) for the superelliptic \( K \)-curve \( y^q = f(x) \) and \( J(C_{f,q}) \) for its Jacobian. Recall that \( J(C_{f,q}) \) is an abelian variety that is defined over \( K \). In [24] I constructed an abelian positive-dimensional \( K \)-subvariety \( J^{(f,q)} \subset J(C_{f,q}) \) that enjoys the following properties.

1. There exists a \( K \)-isogeny of abelian varieties \( \prod_{j=1}^{r} J^{(f,\ell^j)} \to J(C_{f,q}) \).

2. There is a ring embedding \( e_q: \mathbb{Z}[\zeta_q] \hookrightarrow \text{End}_K(J^{(f,q)}) \) that sends 1 to \( 1_{J^{(f,q)}} \) and enjoys the following properties.
   
   (1) \( \delta := e_q(\zeta_q) \in \text{End}_K(J^{(f,q)}) \) is an automorphism of \( J^{(f,q)} \) that satisfies
   \[
   \sum_{i=0}^{\ell-1} \delta^{i\ell^r-1} = 0, \quad \delta^q = 1_{J^{(f,q)}}.
   \]

   (2) If \( l \nmid n \) then the Gal\((K)\)-(sub)module \( (J^{(f,q)})^{\delta} \) of \( \delta \)-invariants is isomorphic to \( \left( \mathbb{F}_\ell^{n/q} \right)^0 \).

   (3) If \( l \nmid n \) then the eigenvalues of \( \delta^*: \Omega^1(J^{(f,q)}) \) are primitive \( q \)th roots of unity. In addition, for each positive integer \( i \) with
   \[
   1 \leq i \leq q, \quad (i, \ell) = 1
   \]
   the multiplicity of \( \zeta^{-i} \) as an eigenvalue of \( \delta^* \) is \( [ni/q] \). In particular, \( \zeta^{-i} \) is an eigenvalue of \( \delta^* \) if and only if \( [ni/q] > 0 \).

Proof of Theorem 1.10. We may assume that \( \ell \) does not divide \( n \), the field \( K \) is perfect and contains a primitive \( q \)th root of unity, and Gal\((f) = A_n \). Since \( J(C_{f,q}) \) is ordinary, it follows from Property (i) that \( J^{(f,\ell^j)} \) is ordinary if \( 1 \leq j \leq r \). Applying Theorem 2.2 to

\[
Y = J^{(f,\ell^j)}, \quad \delta = e_{\ell^j}(\zeta_{\ell^j})
\]

for all such \( j \), we obtain that

\[
\text{End}(J^{(f,\ell^j)}) \cong \mathbb{Z}[\zeta_{\ell^j}], \quad \text{End}^0(J^{(f,\ell^j)}) \cong \mathbb{Q}(\zeta_{\ell^j}).
\]
In particular, all $J^{(f,ℓ_j)}$ are absolutely simple and their endomorphism algebras are non-isomorphic for distinct $j$. Now Property (i) implies that

$$\text{End}^0(J(C_{f,q})) \cong \bigoplus_{j=1}^r \text{End}^0(J^{(f,ℓ_j)}) \cong \bigoplus_{j=1}^r \mathbb{Q}(ζ_{ℓ_j}).$$

This implies that

$$\text{End}^0(J(C_{f,q})) \cong \bigoplus_{j=1}^r \mathbb{Q}(ζ_{ℓ_j}).$$

On the other hand, $\text{End}^0(J(C_{f,q}))$ contains the $\mathbb{Q}$-subalgebra $\mathbb{Q}[δ_q]$ and the latter is isomorphic to $\bigoplus_{j=1}^r \mathbb{Q}(ζ_{ℓ_j})$ (see Subsect. 1.7). Now $\mathbb{Q}$-dimension arguments imply that $\text{End}^0(J(C_{f,q}) = \mathbb{Q}[δ_q]$.

**References**

[1] S. Bosch, W. Lütkebohmert, M. Raynaud: Néron Models. Springer—Verlag, 1990.
[2] G. Faltings, Ch.-L. Chai, Degeneration of abelian varieties. Springer—Verlag, 1990.
[3] W. Messing, The crystals associated to Barsotti–Tate groups with applications to Abelian schemes. Springer Lecture Notes in Math. 264 (1972)
[4] B. Mortimer, The modular permutation representations of the known doubly transitive groups. Proc. London Math. Soc. (3) 41, 1–20 (1980)
[5] D. Mumford, Abelian varieties. 2nd edn. Oxford University Press, London (1974)
[6] D. Mumford, T. Oda, Algebraic Geometry II. Texts and Readings in Mathematics 73, Hindustan Book Agency, 2015.
[7] B. Poonen, E. Schaefer, Explicit descent for jacobians of cyclic covers of the projective line. J. reine angew. Math. 488, 141–188 (1997)
[8] K. Ribet, Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. 98, 751–804 (1976)
[9] E. Schaefer, Computing a Selmer group of a jacobian using functions on the curve. Math. Ann. 310, 447–471 (1998)
[10] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett Publishers, Boston-London (1992)
[11] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton (1971)
[12] J.-P. Serre, J. Tate, Good reduction of abelian varieties. Ann. of Math. 88 (1968), 492–517.
[13] G. Shimura, Abelian varieties with complex multiplication and modular functions. Princeton University Press, Princeton (1997)
[14] J. Xue, Endomorphism algebras of Jacobians of certain superelliptic curves. J. Number Theory 131:2 (2011), 332-342.
[15] J. Xue, C.-F. Yu, Endomorphism algebras of factors of certain hypergeometric Jacobians. Trans. Amer. Math. Soc. 367 (2015), 8071–8106.
[16] N. Yui, On the Jacobian variety of the Fermat curve. J. Algebra 65 (1980), 1–35.
[17] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Res. Letters 7, 123–131 (2000)
[18] Yu. G. Zarhin, Hyperelliptic jacobians and modular representations. In: Moduli of abelian varieties (C. Faber, G. van der Geer, F. Oort, editors). Progress in Math. 195, 473–490. Birkhäuser, Boston (2001)
[19] Yu. G. Zarhin, Endomorphism rings of certain jacobians in finite characteristic. Matem. Sbornik 193, issue 8, 39–48 (2002); Sbornik Math. 193 (8), 1139–1149 (2002).
[20] Yu. G. Zarhin, Cyclic covers, their Jacobians and endomorphisms. J. reine angew. Math. 544, 91–110 (2002).
[21] Yu. G. Zarhin, Hyperelliptic jacobians and simple groups $U_3(2^n)$. Proc. AMS 131, 95–102 (2003)
[22] Yu. G. Zarhin, The endomorphism rings of jacobians of cyclic covers of the projective line. Math. Proc. Cambridge Philos. Soc. 136, 257–267 (2004).
[23] Yu. G. Zarhin, Non-supersingular hyperelliptic jacobians. Bull. Soc. Math. France 132, 617–634 (2004)
[24] Yu. G. Zarhin, Endomorphism algebras of superelliptic Jacobians. In: Geometric methods in Algebra and Number Theory (F. Bogomolov, Yu. Tschinkel, editors). Progress in Math. 235, 339–362, Birkhäuser, Boston Basel Berlin (2005)
[25] Yu. G. Zarhin, *Abelian varieties without homotheties*. Math. Res. Letters 14 (2007), 157–164.
[26] Yu. G. Zarhin, *Superelliptic jacobians*. In: “Diophantine Geometry” Proceedings (U. Zannier, ed.), Edizioni Della Normali, Pisa, pp. 363-390 (2007)
[27] Yu. G. Zarhin, *Endomorphisms of superelliptic jacobians*. Math. Z. 261 (2009), 691–707, 709.
[28] Yu. G. Zarhin, *Endomorphisms of superelliptic jacobians*. arXiv:math/0605028v6 [math.AG].
[29] Yu. G. Zarhin, *Endomorphism Algebras of Abelian Varieties with Special Reference to Superelliptic Jacobians*. In: Geometry, Algebra, Number Theory, and Their Information Technology Applications. Springer Proceedings in Mathematics and Statistics 251 (2018), 477–528.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address: zarhin@math.psu.edu