CYCLIC COVERS OF PRIME POWER DEGREE, JACOBIANS
AND ENDMORPHISMS

YURI G. ZARHIN

Abstract. Suppose $K$ is a field of characteristic zero, $K_a$ is its algebraic
closure, $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$, whose
Galois group coincides either with the full symmetric group $S_n$ or with the
alternating group $A_n$. Let $q$ be a power prime, $P_q(t) = t^q - 1$.

Let $C$ be the superelliptic curve $y^q = f(x)$ and $J(C)$ its jacobian. We
prove that if $p$ does not divide $n$ then the algebra $\text{End}(J(C)) \otimes \mathbb{Q}$ of $K_a$-
edmorphisms of $J(C)$ is canonically isomorphic to $\mathbb{Q}[t]/P_q(t)\mathbb{Q}[t]$.

1. Introduction

We write $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ for the ring of integers, the field of rational numbers and the
field of complex numbers respectively. Recall that a number field is called a CM-
field if it is a purely imaginary quadratic extension of a totally real field. Let $p$
be a prime, $q = p^r$ an integral power of $p$, $\zeta_q \in \mathbb{C}$ 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 $\mathbb{Q}(\zeta_q)$. If $q = 2$
then $\mathbb{Q}(\zeta_q) = \mathbb{Q}$. It is well-known that if $q > 2$ then $\mathbb{Q}(\zeta_q)$ is a CM-field of degree
$(p - 1)p^{r-1}$. Let us put

$$P_q(t) = \frac{t^q - 1}{t - 1} = t^{q-1} + \cdots + 1 \in \mathbb{Z}[t].$$

Clearly,

$$P(t) = \prod_{i=1}^r \Phi_{p^i}(t)$$

where

$$\Phi_{p^i}(t) = t^{(p-1)p^{i-1}} + \cdots + t^{p^{i-1}} + 1 \in \mathbb{Z}[t]$$

is the $p^i$th cyclotomic polynomial. In particular,

$$\mathbb{Q}[t]/\Phi_{p^i}(t)\mathbb{Q}[t] = \mathbb{Q}(\zeta_{p^i})$$

and

$$\mathbb{Q}[t]/P_q(t)\mathbb{Q}[t] = \prod_{i=1}^r \mathbb{Q}(\zeta_{p^i}).$$

We write $\mathbb{F}_p$ for the finite field with $p$ elements.
Let \( f(x) \in \mathbb{C}[x] \) be a polynomial of degree \( n \geq 4 \) without multiple roots. Let \( C_{f,q} \) be a smooth projective model of the smooth affine curve

\[
y^q = f(x).
\]

Throughout this paper we assume that either \( p \) does not divide \( n \) or \( q \) divides \( n \). It is well-known that the genus \( g(C_{f,q}) \) of \( C_{f,q} \) is \((q - 1)(n - 1)/2\) if \( p \) does not divide \( n \) and \((q - 1)(n - 2)/2\) if \( q \) divides \( n \). The map

\[
(x, y) \mapsto (x, \zeta_q y)
\]

gives rise to a non-trivial birational automorphism

\[
\delta_q : C_{f,q} \to C_{f,q}
\]
of period \( q \).

The jacobian \( J(C_{f,q}) \) of \( C_{f,q} \) is an abelian variety of dimension \( g(C_{f,q}) \). We write \( \text{End}(J(C_{f,q})) \) for the ring of endomorphisms of \( J(C_{f,q}) \) over \( \mathbb{C} \) and \( \text{End}^0(J(C_{f,q})) \) for the endomorphism algebra \( \text{End}(J(C_{f,q})) \otimes \mathbb{Q} \). By Albanese functoriality, \( \delta_q \) induces an automorphism of \( J(C_{f,q}) \) which we still denote by \( \delta_q \). One may easily check (see below) that

\[
\delta_q^{-1} + \cdots + \delta_q + 1 = 0
\]
in \( \text{End}(J(C_{f,q})) \). This implies that if \( \mathbb{Q}[\delta_q] \) is the \( \mathbb{Q} \)-subalgebra of \( \text{End}^0(J(C_{f,q})) \) generated by \( \delta_q \) then there is the natural surjective homomorphism

\[
\mathbb{Q}[t]/\mathcal{P}_q(t)\mathbb{Q}[t] \twoheadrightarrow \mathbb{Q}[\delta_q]
\]

which sends \( t + \mathcal{P}_q(t)\mathbb{Q}[t] \) to \( \delta_q \). One may check that this homomorphism is, in fact, an isomorphism (see [9, p. 149], [10, p. 458]) where the case \( q = p \) was treated).

This gives us an embedding

\[
\mathbb{Q}[t]/\mathcal{P}_q(t)\mathbb{Q}[t] \cong \mathbb{Q}[\delta_q] \subset \text{End}^0(J(C_{f,q})).
\]

Our main result is the following statement.

**Theorem 1.1.** Let \( K \) be a subfield of \( \mathbb{C} \) such that all the coefficients of \( f(x) \) lie in \( K \). Assume also that \( f(x) \) is an irreducible polynomial in \( K[x] \) of degree \( n \geq 5 \) and its Galois group over \( K \) is either the symmetric group \( S_n \) or the alternating group \( A_n \). In addition, assume that either \( p \) does not divide \( n \) or \( q \mid n \). Then

\[
\text{End}^0(J(C_{f,q})) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}[t]/\mathcal{P}_q(t)\mathbb{Q}[t] = \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p^r}).
\]
Remark 1.2. In the case when $q$ is a prime (i.e. $q = p$) the assertion of Theorem 1.1 is proven in [16, 23]. See [21, 25, 20] for a discussion of finite characteristic case.

Examples 1.3. Let $n \geq 5$ be an integer, $p$ a prime, $r$ a positive integer, $q = p^r$.

(1) The polynomial $x^n - x - 1 \in \mathbb{Q}[x]$ has Galois group $S_n$ over $\mathbb{Q}$ ([13, p. 42]). Therefore the endomorphism algebra (over $\mathbb{C}$) of the jacobian $J(C)$ of the curve $C : y^q = x^n - x - 1$ is $\mathbb{Q}[t]/P_q(t)\mathbb{Q}[t]$.

(2) The Galois group of the “truncated exponential” $\exp_n(x) := 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!} \in \mathbb{Q}[x]$ is either $S_n$ or $A_n$ [11]. Therefore the endomorphism algebra (over $\mathbb{C}$) of the jacobian $J(C)$ of the curve $C : y^q = \exp_n(x)$ is $\mathbb{Q}[t]/P_q(t)\mathbb{Q}[t]$.

Remark 1.4. If $f(x) \in K[x]$ then the curve $C_{f,q}$ and its jacobian $J(C_{f,q})$ are defined over $K$. Let $K_a \subset \mathbb{C}$ be the algebraic closure of $K$. Clearly, all endomorphisms of $J(C_{f,q})$ are defined over $K_a$. This implies that in order to prove Theorem 1.1 it suffices to check that $\mathbb{Q}[\delta_q]$ coincides with the $\mathbb{Q}$-algebra of $K_a$-endomorphisms of $J(C_{f,q})$.

2. Complex abelian varieties

Throughout this section we assume that $Z$ is a complex abelian variety of positive dimension. As usual, we write $\text{End}^0(Z)$ for the semisimple finite-dimensional $\mathbb{Q}$-algebra $\text{End}(Z) \otimes \mathbb{Q}$. We write $\mathcal{C}_Z$ for the center of $\text{End}^0(Z)$. It is well-known that $\mathcal{C}_Z$ is a direct product of finitely many number fields. All the fields involved are either totally real number fields or CM-fields. Let $H_1(Z, \mathbb{Q})$ be the first rational homology group of $Z$; it is a 2dim($Z$)-dimensional $\mathbb{Q}$-vector space. By functoriality, $\text{End}^0(Z)$ acts on $H_1(Z, \mathbb{Q})$; hence we have an embedding

$$\text{End}^0(Z) \hookrightarrow \text{End}_\mathbb{Q}(H_1(Z, \mathbb{Q}))$$

(which sends 1 to 1).

Suppose $E$ is a subfield of $\text{End}^0(Z)$ that contains the identity map. Then $H_1(Z, \mathbb{Q})$ becomes an $E$-vector space of dimension

$$d = \frac{2\text{dim}(Z)}{[E : \mathbb{Q}]}.$$

We write

$$\text{Tr}_E : \text{End}_E(H_1(Z, \mathbb{Q})) \to E$$
for the corresponding trace map on the $E$-algebra of $E$-linear operators in $H_1(Z, Q)$.

Extending by $C$-linearity the action of $\text{End}^0(Z)$ and of $E$ on the complex cohomology group

$$H_1(Z, Q) \otimes Q C = H_1(Z, C)$$

of $Z$ we get the embeddings

$$E \otimes Q C \subset \text{End}^0(Z) \otimes Q C \hookrightarrow \text{End}_C(H_1(Z, C))$$

which provide $H_1(Z, C)$ with a natural structure of free $E_C := E \otimes Q C$-module of rank $d$. If $\Sigma_E$ is the set of all field embeddings $\sigma : E \hookrightarrow C$ then it is well-known that

$$E_C = E \otimes Q C = \prod_{\sigma \in \Sigma_E} E \otimes E,_{\sigma} C = \prod_{\sigma \in \Sigma_E} C_\sigma$$

where

$$C_\sigma = E \otimes E,_{\sigma} C = C.$$

Since $H_1(Z, C)$ is a free $E_C$-module of rank $d$, there is the corresponding trace map

$$\text{Tr}_{E_C} : \text{End}_{E_C}(H_1(Z, C)) \to E_C$$

which coincides on $E_C$ with multiplication by $d$ and with $\text{Tr}_E$ on $\text{End}_E(H_1(Z, Q))$.

We write $\text{Lie}(Z)$ for the tangent space of $Z$; it is a $\dim(Z)$-dimensional $C$-vector space. By functoriality, $\text{End}^0(Z)$ and therefore $E$ act on $\text{Lie}(Z)$. This provides $\text{Lie}(Z)$ with a natural structure of $E \otimes Q C$-module. We have

$$\text{Lie}(Z) = \bigoplus_{\sigma \in \Sigma_E} C_\sigma \text{Lie}(Z) = \oplus_{\sigma \in \Sigma_E} \text{Lie}(Z)_\sigma$$

where

$$\text{Lie}(Z)_\sigma = C_\sigma \text{Lie}(Z) = \{ x \in \text{Lie}(Z) \mid e x = \sigma(e)x \quad \forall e \in E \}.$$

Let us put

$$n_\sigma = n_\sigma(Z, E) = \dim_{C_\sigma} \text{Lie}(Z)_\sigma = \dim_{C} \text{Lie}(Z)_\sigma.$$

**Remark 2.1.** Let $\Omega^1(Z)$ be the space of the differentials of the first kind on $Z$. It is well-known that the natural map

$$\Omega^1(Z) \to \text{Hom}_C(\text{Lie}(Z), C)$$

is an isomorphism. This isomorphism allows us to define via duality the natural homomorphism

$$E \to \text{End}_C(\text{Hom}_C(\text{Lie}(Z), C)) = \text{End}_C(\Omega^1(Z)).$$
This provides $\Omega^1(Z)$ with a natural structure of $E \otimes_{\mathbb{Q}} \mathbb{C}$-module in such a way that

$$\Omega^1(Z)_\sigma := \mathbb{C}_\sigma \Omega^1(Z) \cong \text{Hom}_{\mathbb{C}}(\text{Lie}(Z)_\sigma, \mathbb{C}).$$

In particular,

$$n_{\sigma} = \dim_{\mathbb{C}}(\text{Lie}(Z)_\sigma) = \dim_{\mathbb{C}}(\Omega^1(Z)_\sigma).$$

**Theorem 2.2.** Suppose that $E$ contains $\mathcal{C}_Z$. Then the tuple

$$(n_{\sigma})_{\sigma \in \Sigma_E} \in \prod_{\sigma \in \Sigma_E} \mathbb{C}_{\sigma} = E \otimes_{\mathbb{Q}} \mathbb{C}$$

lies in $\mathcal{C}_Z \otimes_{\mathbb{Q}} \mathbb{C}$. In particular, if $E/\mathbb{Q}$ is Galois and $\mathcal{C}_Z \neq E$ then there exists a nontrivial automorphism $\kappa : E \to E$ such that $n_{\sigma} = n_{\sigma \kappa}$ for all $\sigma \in \Sigma_E$.

**Proof.** This is Theorem 2.3 of [23].

**Corollary 2.3.** Suppose that there exist a prime $p$, a positive integer $r$, the power prime $q = p^r$ and an integer $n \geq 4$ enjoying the following properties:

(i) $E = \mathbb{Q}(\zeta_q) \subset \mathbb{C}$ where $\zeta_q \in \mathbb{C}$ is a primitive $q$th root of unity;

(ii) $n$ is not divisible by $p$, i.e. $n$ and $q$ are relatively prime;

(iii) Let $i < q$ be a positive integer that is not divisible by $p$ and $\sigma_i : E = \mathbb{Q}(\zeta_q) \hookrightarrow \mathbb{C}$ an embedding that sends $\zeta_q$ to $\zeta_q^{-i}$. Then

$$n_{\sigma_i} = \left\lfloor \frac{ni}{q} \right\rfloor.$$

Then $\mathcal{C}_Z = \mathbb{Q}(\zeta_q)$.

**Proof.** If $q = 2$ then $E = \mathbb{Q}(\zeta_2) = \mathbb{Q}$. Since $\mathcal{C}_Z$ is a subfield of $E = \mathbb{Q}$, we conclude that $\mathcal{C}_Z = \mathbb{Q} = \mathbb{Q}(\zeta_2)$.

So, further we assume that $q > 2$. Clearly, $\{\sigma_i\}$ is the collection $\Sigma$ of all embeddings $\mathbb{Q}(\zeta_q) \hookrightarrow \mathbb{C}$. It is also clear that $n_{\sigma_i} = 0$ if and only if $1 \leq i \leq \left\lfloor \frac{q}{n} \right\rfloor$. Suppose that $\mathcal{C}_Z \neq \mathbb{Q}(\zeta_q)$. It follows from Theorem [23] that there exists a non-trivial field automorphism $\kappa : \mathbb{Q}(\zeta_q) \to \mathbb{Q}(\zeta_q)$ such that for all $\sigma \in \Sigma$

$$n_{\sigma} = n_{\sigma \kappa}.$$

Clearly, there exists an integer $m$ such that $p$ does not divide $m$, $1 < m < q$ and $\kappa(\zeta_q) = \zeta_q^m$.

Assume that $q < n$. In this case the function $i \mapsto n_{\sigma_i} = \left\lfloor \frac{ni}{q} \right\rfloor$ is strictly increasing and therefore $n_{\sigma_i} \neq n_{\sigma_j}$ while $i \neq j$. This implies that $\sigma_i = \sigma_j \kappa$, i.e. $\kappa$ is the identity map which is not the case. The obtained contradiction implies that

$$n < q.$$
Since $n \geq 4$, 

$$q \geq 5.$$ 

Clearly, $n_\sigma = 0$ if and only if $\sigma = \sigma_i$ with $1 \leq i \leq \left[\frac{q}{n}\right]$. Since $n$ and $q$ are relatively prime, $\left[\frac{q}{n}\right] = \left[\frac{q-1}{n}\right]$. It follows that $n_\sigma = 0$ if and only if $1 \leq i \leq \left[\frac{q-1}{n}\right]$. Clearly, the map $\sigma \mapsto \sigma \kappa$ permutes the set $\{\sigma_i \mid 1 \leq i \leq \left[\frac{q-1}{n}\right], p$ does not divide $i\}$.

Since $\kappa(\zeta_q) = \zeta_q^m$, $\sigma_i \kappa(\zeta_q) = \zeta_q^{-im}$. This implies that multiplication by $m$ in $(\mathbb{Z}/q\mathbb{Z})^* = \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ leaves invariant the subset

$$A := \{i \mod q \in \mathbb{Z}/q\mathbb{Z} \mid 1 \leq i \leq \left[\frac{q-1}{n}\right], p$ does not divide $i\}.$$ 

Clearly, $A$ contains 1 and therefore $m = m \cdot 1 \in A$. Since $m < q$,

$$m = m \cdot 1 \leq \left[\frac{(q-1)}{n}\right] \leq \frac{(q-1)}{4}.$$ 

Let us consider the arithmetic progression consisting of $2m$ integers $\left[\frac{(q-1)}{n}\right] + 1, \ldots, \left[\frac{(q-1)}{n}\right] + 2m$ with difference 1. All its elements lie between $\left[\frac{(q-1)}{n}\right] + 1$ and $\left[\frac{(q-1)}{n}\right] + 2m \leq 3 \left[\frac{(q-1)}{n}\right] \leq \frac{3(q-1)}{4} < q - 1$.

Clearly, there exist exactly two elements of $A$ say, $d_1$ and $d_2 = d_1 + m$ that are divisible by $m$. Then there is a positive integer $c_1$ such that

$$d_1 = mc_1, d_2 = m(c_1 + 1).$$

Clearly, either $c_1$ or $c_1 + 1$ is not divisible by $p$; we put $c = c_1$ in the former case and $c = c_1 + 1$ in the latter case. However, $c$ is not divisible by $p$ and

$$\left[\frac{(q-1)}{n}\right] < mc \leq \left[\frac{(q-1)}{n}\right] + 2m < q - 1.$$ 

In particular, $mc$ does not lie in $A$. It follows that $c$ also does not lie in $A$ and therefore

$$c > \left[\frac{(q-1)}{n}\right].$$ 

This means that

$$mc > m \left[\frac{(q-1)}{n}\right].$$ 

Since

$$mc \leq \left[\frac{(q-1)}{n}\right] + 2m,$$

we conclude that

$$(m-1) \left[\frac{(q-1)}{n}\right] < 2m.$$
and therefore
\[ \left\lfloor \frac{(q-1)}{n} \right\rfloor < \frac{2m}{m-1} = 2 + \frac{2}{m-1}. \]
Since
\[ 1 < m < \left\lfloor \frac{(q-1)}{n} \right\rfloor, \]
we conclude that if \( m > 2 \) then \( m \geq 3 \) and
\[ 3 \leq m < \left\lfloor \frac{(q-1)}{n} \right\rfloor < 2 + \frac{2}{m-1} \leq 3 \]
and therefore \( 3 < 3 \) which could not be the case. Hence \( m = 2 \) and
\[ 2 = m < \left\lfloor \frac{(q-1)}{n} \right\rfloor < 2 + \frac{2}{m-1} = 4 \]
and therefore
\[ \left\lfloor \frac{(q-1)}{n} \right\rfloor = 3. \]
It follows that
\[ q \geq 1 + 3n \geq 1 + 3 \cdot 4 = 13. \]
Since \( m = 2 \) is not divisible by \( p \), we conclude that \( p \geq 3 \) and either \( p = 3 \) and \( A = \{1, 2\} \) or \( p > 3 \) and \( A = \{1, 2, 3\} \). In both cases \( 4 = 2 \cdot 2 = m \cdot 2 \) must lie in \( A \).
Contradiction. \( \square \)

3. **Abelian varieties over arbitrary fields**

Let \( K \) be a field. Let us fix its algebraic closure \( K_a \) and denote by \( \text{Gal}(K) \) the absolute Galois group \( \text{Aut}(K_a/K) \) of \( K \). If \( X \) is an abelian variety over \( K_a \) then we write \( \text{End}(X) \) for the ring of all its \( K_a \)-endomorphisms. We write \( 1_X \) (or even just 1) for the identity automorphism of \( X \). If \( Y \) is (may be another) abelian variety over \( K_a \) then we write \( \text{Hom}(X,Y) \) for the group of all \( K_a \)-homomorphisms from \( X \) to \( Y \).

It is well-known that \( \text{Hom}(X,Y) = 0 \) if and only if \( \text{Hom}(Y,X) = 0 \). One may easily check that if \( X \) is simple and \( \text{dim}(X) \geq \text{dim}(Y) \) then \( \text{Hom}(X,Y) = 0 \) if and only if \( X \) and \( Y \) are not isogenous over \( K_a \). We write \( \text{End}^0(X) \) for the finite-dimensional semisimple \( \mathbb{Q} \)-algebra \( \text{End}(X) \otimes \mathbb{Q} \) and \( \text{Hom}^0(X,Y) \) for the finite-dimensional \( \mathbb{Q} \)-vector space \( \text{Hom}(X,Y) \otimes \mathbb{Q} \). Clearly, if \( X = Y \) then
\[ \text{End}^0(X) = \text{Hom}^0(X,Y) = \text{Hom}^0(Y,X) = \text{End}^0(Y). \]

It is well-known that \( \text{Hom}^0(X,Y) \) and \( \text{Hom}^0(Y,X) \) have the same dimension which does not exceed \( 4\text{dim}(X)\text{dim}(Y) \) \[16\]. The equality holds if and only if \( \text{char}(K) > 0 \) and both \( X \) and \( Y \) are supersingular abelian varieties \[16\] \[22\].
It is well-known that if $X$ and $Y$ are simple and the $\mathbb{Q}$-algebras $\text{End}^0(X)$ and $\text{End}^0(Y)$ are not isomorphic then

$$\text{Hom}(X, Y) = 0, \text{Hom}(Y, X) = 0.$$ 

Let $E$ be a number field and $\mathcal{O} \subset E$ be the ring of all its algebraic integers. Let $(X, i)$ be a pair consisting of an abelian variety $X$ over $K_0$ and an embedding

$$i : E \hookrightarrow \text{End}^0(X)$$

Here $1 \in E$ must go to $1_X$. It is well known [7] that the degree $[E : \mathbb{Q}]$ divides $2\dim(X)$, i.e.

$$r = r_X := \frac{2\dim(X)}{[E : \mathbb{Q}]}$$

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. If $Y$ is (possibly) another abelian variety over $K_0$ and $j : E \hookrightarrow \text{End}^0(Y)$ is an embedding that sends 1 to the identity automorphism of $Y$ then we write

$$\text{Hom}^0((X, i), (Y, j)) = \{u \in \text{Hom}^0(X, Y) \mid ui(c) = j(c)u \quad \forall c \in E\}.$$ 

Clearly, $\text{End}^0(X, i) = \text{Hom}^0((X, i), (X, i))$. If $d$ is a positive integer then we write $i^{(d)}$ for the composition

$$E \hookrightarrow \text{End}^0(X) \subset \text{End}^0(X^d)$$

of $i$ and the diagonal inclusion $\text{End}^0(X) \subset \text{End}^0(X^d)$.

**Remark 3.1.** (i) The $E$-algebra $\text{End}^0(X, i)$ is semisimple. Indeed, let us split the semisimple $\mathbb{Q}$-algebra $\text{End}^0(X)$ into a finite direct product

$$\text{End}^0(X) = \prod_s D_s$$

of simple $\mathbb{Q}$-algebras $D_s$. If $\text{pr}_s : \text{End}^0(X) \rightarrow D_s$ is the corresponding projection map and $D_{s, E}$ is the centralizer of $\text{pr}_s i(E)$ in $D_s$ then one may easily check that

$$\text{End}^0(X, i) = \prod_s D_{s, E}.$$ 

Clearly, $\text{pr}_s i(E) \cong E$ is a simple $\mathbb{Q}$-algebra. It follows from Theorem 4.3.2 on p. 104 of [1] that $D_{s, E}$ is also a simple $\mathbb{Q}$-algebra. This implies easily that $D_{s, E}$ is a simple $E$-algebra and therefore $\text{End}^0(X, i)$ is a semisimple
E-algebra. It is also clear that $\text{End}^0(X, i)$ is a simple $E$-algebra if and only if $\text{End}^0(X)$ is a simple $\mathbb{Q}$-algebra, i.e., $X$ is isogenous to a self-product of (absolutely) simple abelian variety.

(ii) Let $e_s$ be the identity element of $D_s$. One may view $e_s$ as an idempotent in $\text{End}^0(X)$. Clearly,

$$1 = \sum_s e_s$$

in $\text{End}^0(X)$ and $e_s e_t = 0$ if $s \neq t$. There exists a positive integer $N$ such that all $N \cdot e_s$ lie in $\text{End}(X)$. We write $X_s$ for the image

$$X_s := (N e_s)(X);$$

it is an abelian subvariety in $X$ of positive dimension. Clearly, the sum map

$$\pi_X : \prod_s X_s \rightarrow X, \quad (x_s) \mapsto \sum_s x_s$$

is an isogeny. It is also clear that the intersection $D_s \cap \text{End}(X)$ leaves $X_s \subset X$ invariant. This gives us a natural identification

$$D_s \cong \text{End}^0(X_s).$$

One may easily check that each $X_s$ is isogenous to a self-product of (absolutely) simple abelian variety. It is also clear that

$$\text{Hom}(X_s, X_t) = 0 \quad \forall s \neq t.$$ 

We write $i_s$ for the composition

$$\text{pr}_s i : E \hookrightarrow \text{End}^0(X) : D_s \cong \text{End}^0(X_s).$$

Clearly,

$$D_{s, E} = \text{End}^0(X_s, i_s)$$

and

$$\pi_X^{-1} i \pi_X : E \rightarrow \prod_s D_s = \prod_s \text{End}^0(X_s) \subset \text{End}^0(\prod_s X_s).$$

It is also clear that

$$\text{End}^0(\prod_s X_s, \prod_s i_s) = \prod_s D_{s, E}.$$

**Theorem 3.2.**

(i)

$$\dim_E(\text{End}^0((X, i))) \leq \frac{4 \cdot \dim(X)^2}{[E: \mathbb{Q}]^2};$$
(ii) Suppose that
$$\dim_E(\text{End}^0((X, i))) = \frac{4 \cdot \dim(X)^2}{[E : \mathbb{Q}]^2}.$$ Then $X$ is isogenous to a self-product of (absolutely) simple abelian variety. Also $\text{End}^0((X, i))$ is a central simple $E$-algebra, i.e., $E$ coincides with the center of $\text{End}^0((X, i))$. In addition, $X$ is an abelian variety of CM-type.

If $\text{char}(K_a) = 0$ then $[E : \mathbb{Q}]$ is even and there exist a $\frac{[E : \mathbb{Q}]}{2}$-dimensional abelian variety $Z$, an isogeny $\psi : Z^r \to X$, an embedding $k : E \hookrightarrow \text{End}^0(Z)$ that sends $1$ to $1_Z$ and such that
$$\psi \in \text{Hom}^0((Z^r, k^{(r)}), (X, i)).$$

Proof. Recall that $r = 2\dim(X)/[E : \mathbb{Q}]$.

First, assume that $X$ is isogenous to a self-product of (absolutely) simple abelian variety, i.e., $\text{End}^0(X, i)$ is a simple $E$-algebra. We need to prove that
$$N := \dim_E(\text{End}^0(X, i)) \leq r^2.$$ Let $E'$ be the center of $\text{End}^0(X, i)$. Let us put
$$e = [E' : E].$$ Then $\text{End}^0(X, i)$ is a central simple $E'$-algebra of dimension $N/e$. Then there exists a central division $E'$-algebra $D$ such that $\text{End}^0(X, i)$ is isomorphic to the matrix algebra $M_m(D)$ of size $m$ for some positive integer $m$. Dimension arguments imply that
$$m^2 \dim_{E'}(D) = \frac{N}{e}, \quad \dim_{E'}(D) = \frac{N}{em^2}.$$ Since $\dim_{E'}(D)$ is a square,
$$\frac{N}{e} = N_1^2, \quad N = eN_1^2, \quad \dim_{E'}(D) = \left( \frac{N_1}{m} \right)^2$$ for some positive integer $N_1$. Clearly, $m$ divides $N_1$.

Clearly, $D$ contains a (maximal) field extension $L/E'$ of degree $N_1/m$ and $\text{End}^0(X, i) \cong M_m(D)$ contains every field extension $T/L$ of degree $m$. This implies that
$$\text{End}^0(X) \supset \text{End}^0(X, i) \supset T$$ and the number field $T$ has degree
$$[T : \mathbb{Q}] = [E' : \mathbb{Q}] \cdot \frac{N_1}{m} \cdot m = [E : \mathbb{Q}]eN_1.$$
But \([T : \mathbb{Q}]\) must divide \(2\dim(X)\); if the equality holds then \(X\) is an abelian variety of CM-type. This implies that \(eN_1\) divides \(r = \frac{2\dim(X)}{[E : \mathbb{Q}]}\). It follows that \((eN_1)^2\) divides \(r^2\); if the equality holds then \(X\) is an abelian variety of CM-type. But

\[(eN_1)^2 = e^2N_1^2 = e(eN_1^2) = eN = e \cdot \dim_E(\text{End}^0(X, i)).\]

This implies that

\[\dim_E(\text{End}^0(X, i)) \leq \frac{r^2}{e} \leq r^2.\]

If the equality \(\dim_E(\text{End}^0(X, i)) = r^2\) holds then \(e = 1\) and

\[(eN_1)^2 = r^2, N_1 = r, [T : \mathbb{Q}] = [E : \mathbb{Q}]eN_1 = [E : \mathbb{Q}]r = 2\dim(X);\]

in particular, \(X\) is an abelian variety of CM-type. In addition, since \(e = 1\), we have \(E' = E\), i.e. \(\text{End}^0(X, i)\) is a central simple \(E\)-algebra.

Clearly, there exists an abelian variety \(Z\) over \(K_a\) with

\[E \subset D \subset \text{End}^0(Z)\]

and an isogeny

\[\psi : Z^m \to X\]

such that the induced isomorphism

\[\text{End}^0(Z^m) \cong \text{End}^0(X), u \mapsto \psi u \psi^{-1}\]

maps identically

\[E \subset \text{End}^0(Z) \subset \text{End}^0(Z^m)\]

onto \(E \subset \text{End}^0(X)\).

We still have to check that if \(\text{char}(K) = 0\) then

\[2\dim(Z) = [E : \mathbb{Q}].\]

Indeed, since \(D\) is a division algebra, \(\dim_{\mathbb{Q}}(D)\) must divide \(2\dim(Z) = \frac{2\dim(X)}{m} = [E : \mathbb{Q}] \frac{r}{m}\). On the other hand,

\[\dim_{\mathbb{Q}}(D) = [E : \mathbb{Q}] \dim_E(D) = [E : \mathbb{Q}] \left(\frac{r}{m}\right)^2.\]

Since \(m\) divides \(r\), we conclude that \(\frac{r}{m} = 1\), i.e.

\[\dim_E(D) = 1, \quad D = E, \quad 2\dim(Z) = [E : \mathbb{Q}].\]
Now let us consider the case of arbitrary $X$. Applying the already proven case of the theorem to each $X_s$, we conclude that

$$\dim_E(\text{End}^0(X, i)) \leq \left( \frac{2\dim(X_s)}{|E : \mathbb{Q}|} \right)^2.$$ 

Since

$$\text{End}^0(X, i) = \prod_s \text{End}^0(X_s, i_s),$$

we conclude that $\dim_E(\text{End}^0(X, i))$ does not exceed

$$\sum_s \left( \frac{2\dim(X_s)}{|E : \mathbb{Q}|} \right)^2 = \frac{(2\sum_s \dim(X_s))^2}{|E : \mathbb{Q}|^2} = \frac{(2\dim(X))^2}{|E : \mathbb{Q}|^2}.$$ 

It follows that if the equality

$$\dim_E(\text{End}^0(X, i)) = \frac{(2\dim(X))^2}{|E : \mathbb{Q}|^2}$$

holds then the set of indices $s$ is a singleton, i.e. $X = X_s$ is isogenous to a self-product of (absolutely) simple abelian variety. □

Let $d$ be a positive integer that is not divisible by char($K$). Let $X$ be an abelian variety of positive dimension defined over $K$. We write $X_d$ for the kernel of multiplication by $d$ in $X(K_a)$. It is known \[6\] that the commutative group $X_d$ is a free $\mathbb{Z}/d\mathbb{Z}$-module of rank $2\dim(X)$. Clearly, $X_d$ is a Galois submodule in $X(K_a)$. We write

$$\tilde{\rho}_{d,X} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X_d) \cong \text{GL}(2\dim(X), \mathbb{Z}/d\mathbb{Z})$$

for the corresponding (continuous) homomorphism defining the Galois action on $X_d$. Let us put

$$\tilde{G}_{d,X} = \tilde{\rho}_{d,X}(\text{Gal}(K)) \subset \text{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X_d).$$

Clearly, $\tilde{G}_{d,X}$ coincides with the Galois group of the field extension $K(X_d)/K$ where $K(X_d)$ is the field of definition of all points on $X$ of order dividing $d$. In particular, if a prime $\ell \neq \text{char}(K)$ then $X_{\ell}$ is a $2\dim(X)$-dimensional vector space over the prime field $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$ and the inclusion $\tilde{G}_{\ell,X} \subset \text{Aut}_{\mathbb{F}_\ell}(X_{\ell})$ defines a faithful linear representation of the group $\tilde{G}_{\ell,X}$ in the vector space $X_{\ell}$.

We write $\text{End}_K(X) \subset \text{End}(X)$ for the (sub)ring of all $K$-endomorphisms of $X$.

Now let us assume that

$$i(\emptyset) \subset \text{End}_K(X).$$
Let $\lambda$ be a maximal ideal in $\mathcal{O}$. We write $k(\lambda)$ for the corresponding (finite) residue field. Let us put

$$X_\lambda := \{ x \in X(K_a) \mid i(e)x = 0 \quad \forall e \in \lambda \}.$$ 

Clearly, if $\text{char}(k(\lambda)) = \ell$ then $\lambda \supset \ell \cdot \mathcal{O}$ and therefore $X_\lambda \subset X_\ell$. Clearly, $X_\lambda$ is a Galois submodule of $X_\ell$. It is also clear that $X_\lambda$ carries a natural structure of $\mathcal{O}/\lambda = k(\lambda)$-vector space. 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 $X_\lambda$. 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 $K(X_\lambda) = K(X_{\lambda,i})$ is the field of definition of all points in $X_\lambda$.

In order to describe $\tilde{\rho}_{\lambda,X}$ explicitly, let us assume for the sake of simplicity 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

$$[E : \mathbb{Q}] = b \cdot [k(\lambda) : \mathbb{F}_\ell].$$

Then $\mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_\lambda$ where $\mathcal{O}_\lambda$ is the completion of $\mathcal{O}$ with respect to $\lambda$-adic topology. It is well-known that that $\mathcal{O}_\lambda$ is a local principal ideal domain and its only maximal ideal is $\lambda \mathcal{O}_\lambda$. One may easily check that $\ell \cdot \mathcal{O}_\lambda = (\lambda \mathcal{O}_\lambda)^b$.

Let us choose an element $c \in \lambda$ that does not lie in $\lambda^2$. Clearly, $\lambda \mathcal{O}_\lambda = c \cdot \mathcal{O}_\lambda$. This implies that there exists a unit $u \in \mathcal{O}_\lambda^*$ such that $\ell = uc^b$. It follows from the unique factorization of ideals in $\mathcal{O}$ that

$$\lambda = \ell \cdot \mathcal{O} + c \cdot \mathcal{O}.$$ 

It follows readily that

$$X_\lambda = \{ x \in X_\ell \mid cx = 0 \} \subset X_\ell.$$ 

Let $T_\ell(X)$ be the $\mathbb{Z}_\ell$-Tate module of $X$ defined as projective limit of Galois modules $X_{\ell^m}$ where the transition map(s) $X_{\ell^{m+1}} \to X_{\ell^m}$ is multiplication by $\ell$. 


Recall that $T_\ell(X)$ is a free $\mathbb{Z}_\ell$-module of rank $2\dim(X)$ provided with the continuous action

$$\rho_{\ell,X} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(X))$$

and the natural embedding

$$\text{End}_K(X) \otimes \mathbb{Z}_\ell \hookrightarrow \text{End}_{\mathbb{Z}_\ell}(T_\ell(X)),$$

whose image commutes with $\rho_{\ell,X} (\text{Gal}(K))$. In particular, $T_\ell(X)$ carries the natural structure of $\mathbb{O} \otimes \mathbb{Z}_\ell = \mathbb{O}_\lambda$-module; it is known [7] that the $\mathbb{O}_\lambda$-module $T_\ell(X)$ is free of rank $r = r_X = \frac{2\dim(X)}{|E : \mathbb{Q}|}$. There is also the natural isomorphism of Galois modules

$$X_\ell = T_\ell(X)/\ell T_\ell(X),$$

which is also an isomorphism of $\text{End}_K(X) \supset \mathbb{O}$-modules. This implies that the $\mathbb{O}[\text{Gal}(K)]$-module $X_\lambda$ coincides with

$$c^{-1}T_\ell(X)/\ell T_\ell(X) = c^{b-1}T_\ell(X)/c^{b}T_\ell(X) = T_\ell(X)/cT_\ell(X) = T_\ell(X)/\lambda T_\ell(X) = T_\ell(X)/(\lambda \mathbb{O}_\lambda) T_\ell(X).$$

Hence

$$X_\lambda = T_\ell(X)/(\lambda \mathbb{O}_\lambda) T_\ell(X) = T_\ell(X) \otimes_{\mathbb{O}_\lambda} k(\lambda).$$

It follows that

$$\dim_{k(\lambda)} X_\lambda = \frac{2\dim(X)}{|E : \mathbb{Q}|} := r_X.$$

Let us put

$$V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell;$$

it is a $2\dim(X)$-dimensional $\mathbb{Q}_\ell$-vector space that carries a natural structure of $r_X$-dimensional $E_\lambda$-vector space. There is the natural embedding

$$\text{End}(X) \otimes \mathbb{Z}_\ell \hookrightarrow \text{End}_{\mathbb{Q}_\ell}(V_\ell(X)).$$

Extending it by $\mathbb{Q}$-linearity, we get the natural embedding

$$\text{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \text{End}_{\mathbb{Q}_\ell}(V_\ell(X)).$$

Further we will identify $\text{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ with its image in $\text{End}_{\mathbb{Q}_\ell}(V_\ell(X))$.

**Remark 3.3.** Notice that

$$E_\lambda = E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathbb{O} \otimes \mathbb{Q}_\ell = \mathbb{O}_\lambda \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

is the field coinciding with the completion of $E$ with respect to $\lambda$-adic topology. Clearly, $V_\ell(X)$ carries a natural structure of $r_X$-dimensional $E_\lambda$-vector space. One
may easily check that $\text{End}_0^0(X, i) \otimes \mathbb{Q}_\ell$ is a $E \otimes \mathbb{Q}_\ell = E_\lambda$-vector subspace (even subalgebra) in $\text{End}_{E_\lambda}(V_\ell(X))$. Clearly,

$$\dim_{E_\lambda}(\text{End}_0^0(X, i) \otimes \mathbb{Q}_\ell) = \dim_E(\text{End}_0^0(X, i))$$

and

$$\dim_{E_\lambda}(\text{End}_{E_\lambda}(V_\ell(X))) = r_X^2.$$ This implies that

$$\text{End}_0^0(X, i) \otimes \mathbb{Q}_\ell = \text{End}_{E_\lambda}(V_\ell(X))$$

if and only if

$$\dim_E(\text{End}_0^0(X, i)) = r_X^2.$$

Using the inclusion

$$\text{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \subset \text{Aut}_{\mathbb{Q}_\ell}(V_\ell(X)),$$

one may view $\rho_{\ell,X}$ as $\ell$-adic representation

$$\rho_{\ell,X} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \subset \text{Aut}_{\mathbb{Q}_\ell}(V_\ell(X)).$$

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

$$\sigma u(x) = \sigma u(\sigma^{-1} x) \quad \forall x \in X(K_a).$$

Clearly,

$$\sigma u = u \quad \forall u \in \text{End}_K(X).$$

In particular,

$$\sigma u = u \quad \forall u \in \mathcal{O}$$

(here we identify $\mathcal{O}$ with $i(\mathcal{O})$). It follows easily that for each $\sigma \in \text{Gal}(K)$ the map $u \to \sigma u$ extends by $\mathbb{Q}$-linearity to a certain automorphism of $\text{End}_0^0(X)$. It is also clear that $\sigma u = u$ for each $u \in E$ and

$$\sigma u \in \text{End}_0^0(X, i) \quad \forall u \in \text{End}_0^0(X, i), \sigma \in \text{Gal}(K).$$

**Remark 3.4.** The definition of $T_\ell(X)$ as the projective limit of Galois modules $X_{e_m}$ implies that

$$\sigma u(x) = \rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1}(x) \quad \forall x \in T_\ell(X).$$

It follows easily that

$$\sigma u(x) = \rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1}(x) \quad \forall x \in V_\ell(X), u \in \text{End}_0^0(X), \sigma \in \text{Gal}(K).$$
This implies that for each $\sigma \in \text{Gal}(K)$

$$\rho_{\ell,X}(\sigma) \in \text{Aut}_{E_{\lambda}}(V_{\lambda}(X)).$$

and therefore

$$\rho_{\ell,X}(\text{Gal}(K)) \subset \text{Aut}_{E_{\lambda}}(V_{\lambda}(X)).$$

It is also clear that

$$\rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1} \in \text{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell} \quad \forall u \in \text{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$$

and

$$\rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1} \in \text{End}^0(X,i) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell} \quad \forall u \in \text{End}^0(X,i) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}.$$

We refer to [17, 18, 21, 24] for a discussion of the following definition.

**Definition 3.5.** Let $V$ be a vector space over a field $F$, let $G$ be a group and $\rho : G \to \text{Aut}_F(V)$ a linear representation of $G$ in $V$. We say that the $G$-module $V$ is very simple if it enjoys the following property:

If $R \subset \text{End}_F(V)$ is an $F$-subalgebra containing the identity operator $\text{Id}$ such that

$$\rho(\sigma)R\rho(\sigma)^{-1} \subset R \quad \forall \sigma \in G$$

then either $R = F \cdot \text{Id}$ or $R = \text{End}_F(V)$.

**Remarks 3.6.**

(i) If $G'$ is a subgroup of $G$ and the $G'$-module $V$ is very simple then obviously the $G$-module $V$ is also very simple.

(ii) Clearly, the $G$-module $V$ is very simple if and only if the corresponding $\rho(G)$-module $V$ is very simple. This implies easily that if $H \to G$ is a surjective group homomorphism then the $G$-module $V$ is very simple if and only if the corresponding $H$-module $V$ is very simple.

(iii) Let $G'$ be a normal subgroup of $G$. If $V$ is a very simple $G$-module then either $\rho(G') \subset \text{Aut}_k(V)$ consists of scalars (i.e., lies in $k \cdot \text{Id}$) or the $G'$-module $V$ is absolutely simple. See [21, Remark 5.2(iv)].

(iv) Suppose $F$ is a discrete valuation field with valuation ring $O_F$, maximal ideal $m_F$ and residue field $k = O_F/m_F$. Suppose $V_F$ a finite-dimensional $F$-vector space, $\rho_F : G \to \text{Aut}_F(V_F)$ a $F$-linear representation of $G$. Suppose $T$ is a $G$-stable $O_F$-lattice in $V_F$ and the corresponding $k[G]$-module $T/m_FT$ is isomorphic to $V$. Assume that the $G$-module $V$ is very simple. Then the $G$-module $V_F$ is also very simple. See [21, Remark 5.2(v)].
Theorem 3.7. Suppose that $X$ is an abelian variety defined over $K$ and $i(\mathcal{O}) \subset \text{End}_K(X)$. Let $\ell$ be a prime different from $\text{char}(K)$. Suppose that $\lambda$ is the only maximal ideal dividing $\ell$ in $\mathcal{O}$. Suppose that the natural representation in the $k(\lambda)$-vector space $X_\lambda$ is very simple. Then $\text{End}^0(X,i)$ enjoy one of the following two properties:

(i) $\text{End}^0(X,i) = i(E)$, i.e. $i(E) \cong E$ is a maximal commutative subalgebra in $\text{End}^0(X)$ and $i(\mathcal{O}) \cong \mathcal{O}$ is a maximal commutative subring in $\text{End}(X)$;

(ii) $\text{End}^0(X,i)$ is a central simple $E$-algebra of dimension $r_X^2$ and $X$ is an abelian variety of CM-type over $K_a$. In addition, if $\text{char}(K) = 0$ then $[E : \mathbb{Q}]$ is even and there exist a $\frac{[E : \mathbb{Q}]}{2}$-dimensional abelian variety $Z$, an isogeny $\psi : Z^r \to X$ and an embedding $k : E \to \text{End}^0(Z)$ that sends 1 to $1_Z$ such that

$$\psi \in \text{Hom}^0((Z^r,k(r)),(X,i)).$$

Proof. In light of 3.6(ii), the $\text{Gal}(K)$-module $X_\lambda$ is very simple. In light of 3.6(iv) and Remark 3.4

$$\rho_{\ell,X} : \text{Gal}(K) \to \text{Aut}_{E_\lambda}(V_\ell(X))$$

is also very simple. Let us put

$$R = \text{End}^0(X,i) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$ 

It follows from Remark 3.4 that either $R = E_\lambda \text{Id}$ or $R = \text{End}_{E_\lambda}(V_\ell(X))$. By Remark 3.5

$$\dim_{E_\lambda}(R) = \dim_{E_\lambda}(\text{End}^0(X,i) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) = \dim_E(\text{End}^0(X,i)).$$

It follows that $\dim_E(\text{End}^0(X,i)) = 1$ or $r_X^2$. Clearly, if $\dim_E(\text{End}^0(X,i)) = 1$ then $\text{End}^0(X,i) = i(E)$ and the property (i) holds. Suppose that $\dim_E(\text{End}^0(X,i)) = r_X^2$. Applying Theorem 3.2 we conclude that the property (ii) holds. □

Let $Y$ be an abelian variety of positive dimension over $K_a$ and $u$ a non-zero endomorphism of $Y$. Let us consider the abelian (sub)variety

$$Z = u(Y) \subset Y.$$
Remark 3.8. If \( Y \) is defined over \( K \) and \( u \in \text{End}_K(Y) \) then \( Z \) is also defined over \( K \) and the inclusion map \( Z \subset Y \) is defined over \( K \). Indeed, clearly, \( Z \) and the inclusion map \( Z \subset Y \) are defined over \( K_{\text{Gal}(K)} \), i.e. \( Z \) and \( Z \subset Y \) are defined over a purely inseparable extension of \( K \). By Theorem of Chow [3, Th. 5 on p. 26], \( Z \) is defined over \( K \). It follows that every homomorphism between \( Z \) and \( Y \) is defined over a separable extension of \( K \). Hence \( Z \subset Y \) is defined over \( K \).

We write \( \Omega^1(Y) \) (resp. \( \Omega^1(Z) \)) for the \( \dim(Y) \)-dimensional (resp. \( \dim(Z) \)-dimensional) \( K \)-vector space of differentials of the first kind on \( Y \) (resp. on \( Z \)).

Theorem 3.9. Let \( Y \) be an abelian variety of positive dimension over \( K \) and \( \delta \) an automorphism of \( Y \). Suppose that the induced \( K \)-linear operator

\[ \delta^* : \Omega^1(Y) \to \Omega^1(Y) \]

is diagonalizable. Let \( S \) be the set of eigenvalues of \( \delta^* \) and \( \text{mult}_Y : S \to \mathbb{Z}_+ \) the integer-valued function which assigns to each eigenvalue its multiplicity.

Suppose that \( P(t) \) is a polynomial with integer coefficients such that \( u = P(\delta) \) is a non-zero endomorphism of \( Y \). Let us put \( Z = u(Y) \). Clearly, \( Z \) is \( \delta \)-invariant and we write \( \delta_Z : Z \to Z \) for the corresponding automorphism of \( Z \) (i.e. for the restriction of \( \delta \) to \( Z \)).

Suppose that

\[ \dim(Z) = \sum_{\lambda \in S, P(\lambda) \neq 0} \text{mult}_Y(\lambda). \]

Then the spectrum of \( \delta^*_Z : \Omega^1(Z) \to \Omega^1(Z) \) coincides with \( S_P = \{ \lambda \in S, P(\lambda) \neq 0 \} \) and the multiplicity of an eigenvalue \( \lambda \) of \( \delta^*_Z \) equals \( \text{mult}_Y(\lambda) \).

Proof. Clearly, \( u \) commutes with \( \delta \). We write \( v \) for the (surjective) homomorphism \( Y \to Z \) induced by \( u \) and \( j \) for the inclusion map \( Z \subset Y \). Notice that \( u : Y \to Y \) splits into a composition

\[ Y \xrightarrow{v} Z \xrightarrow{j} Y, \]

i.e. \( u = jv \). Clearly,

\[ \delta_Z v = v \delta \in \text{Hom}(Y, Z), \quad j \delta_Z = \delta j \in \text{Hom}(Z, Y), \quad u = jv \in \text{End}(Y), \quad u \delta = \delta u \in \text{End}(Y). \]

It is also clear that the induced map

\[ u^* : \Omega^1(Y) \to \Omega^1(Y) \]

coincides with \( P(\delta^*) \). It follows that

\[ u^*(\Omega^1(Y)) = P(\delta^*)(\Omega^1(Y)) \]
has dimension
\[ \sum_{\lambda \in S, P(\lambda) \neq 0} \text{mult}_Y(\lambda) = \dim(Y) \]
and coincides with
\[ \oplus_{\lambda \in S, P(\lambda) \neq 0} W_\lambda \]
where \( W_\lambda \) is the eigenspace of \( \delta \) attached to eigenvalue \( \lambda \). Since \( u^* = v^* j^* \),
\[ u^*(\Omega^1(Y)) = v^* j^*(\Omega^1(Y)) \subset v^*(\Omega^1(Z)). \]
Since
\[ \dim(u^*(\Omega^1(Y))) = \dim(Y) = \dim(\Omega^1(Z)) \geq \dim(v^*(\Omega^1(Z))), \]
the subspace
\[ u^*(\Omega^1(Y)) = v^*(\Omega^1(Z)) \]
and
\[ v^* : \Omega^1(Z) \hookrightarrow \Omega^1(Y). \]
It follows that if we denote by \( w \) the isomorphism \( v^* : \Omega^1(Z) \cong v^*(\Omega^1(Z)) \) and by \( \gamma \) the restriction of \( \delta^* \) to \( v^*(\Omega^1(Z)) \) then \( \gamma w = w \delta_Y^* \) and therefore
\[ \gamma = w \delta_Y^* w^{-1}. \]

\[ \square \]

4. Cyclic covers and Jacobians

Throughout this paper we fix a prime number \( p \) and its integral power \( q = p^r \) and assume that \( K \) is a field of characteristic different from \( p \). We fix an algebraic closure \( K_a \) and write \( \text{Gal}(K) \) for the absolute Galois group \( \text{Aut}(K_a/K) \). We also fix in \( K_a \) a primitive \( q \)th root of unity \( \zeta \).

Let \( f(x) \in K[x] \) be a separable polynomial of degree \( n \geq 4 \). We write \( \mathfrak{R}_f \) for the set of its roots and denote by \( L = L_f = K(\mathfrak{R}_f) \subset K_a \) the corresponding splitting field. As usual, the Galois group \( \text{Gal}(L/K) \) is called the Galois group of \( f \) and denoted by \( \text{Gal}(f) \). Clearly, \( \text{Gal}(f) \) permutes elements of \( \mathfrak{R}_f \) and the natural map of \( \text{Gal}(f) \) into the group \( \text{Perm}(\mathfrak{R}_f) \) of all permutations of \( \mathfrak{R}_f \) is an embedding. We will identify \( \text{Gal}(f) \) with its image and consider it as a permutation group of \( \mathfrak{R}_f \).

Clearly, \( \text{Gal}(f) \) is transitive if and only if \( f \) is irreducible in \( K[x] \).

Further, we assume that either \( p \) does not divide \( n \) or \( q \) does divide \( n \).

If \( p \) does not divide \( n \) then we write (as in [19])
\[ V_{f,p} = (F_p^{\mathfrak{R}_f})^0 = (F_p^{\mathfrak{R}_f})^0 \]
for the \((n - 1)\)-dimensional \(\mathbb{F}_p\)-vector space of functions
\[
\phi : \mathfrak{R}_f \to \mathbb{F}_p, \quad \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = 0
\]
provided with a natural action of the permutation group \(\text{Gal}(f) \subset \text{Perm}(\mathfrak{R}_f)\). It is the heart over the field \(\mathbb{F}_p\) of the group \(\text{Gal}(f)\) acting on the set \(\mathfrak{R}_f\).

**Remark 4.1.** If \(p\) does not divide \(n\) and \(\text{Gal}(f) = S_n\) or \(A_n\) then the \(\text{Gal}(f)\)-module \(V_{f,p}\) is very simple.

Let \(C = C_{f,q}\) be the smooth projective model of the smooth affine \(K\)-curve
\[
y^q = f(x)
\]
So \(C\) is a smooth projective curve defined over \(K\). The rational function \(x \in K(C)\) defines a finite cover \(\pi : C \to \mathbb{P}^1\) of degree \(p\). Let \(B' \subset C(K_a)\) be the set of ramification points. Clearly, the restriction of \(\pi\) to \(B'\) is an injective map \(B' \hookrightarrow \mathbb{P}^1(K_a)\), whose image is the disjoint union of \(\infty\) and \(\mathfrak{R}_f\) if \(p\) does not divide \(\deg(f)\) and just \(\mathfrak{R}_f\) if it does. We write
\[
B = \pi^{-1}(\mathfrak{R}_f) = \{(\alpha, 0) \mid \alpha \in \mathfrak{R}_f\} \subset B' \subset C(K_a).
\]
Clearly, \(\pi\) is ramified at each point of \(B\) with ramification index \(q\). We have \(B' = B\) if and only if \(n\) is divisible by \(p\). If \(n\) is not divisible by \(p\) then \(B'\) is the disjoint union of \(B\) and a single point \(\infty' : = \pi^{-1}(\infty)\). In addition, the ramification index of \(\pi\) at \(\pi^{-1}(\infty)\) is also \(q\). Using Hurwitz’s formula, one may easily compute the genus \(g = g(C) = g(C_{q,f})\) of \(C\) ([24 pp. 401–402], [14 proposition 1 on p. 3359], [9 p. 148]). Namely, \(g\) is \((q - 1)(n - 1)/2\) if \(p\) does not divide \(n\) and \((q - 1)(n - 2)/2\) if \(q\) does divide \(n\).

**Remark 4.2.** Assume that \(p\) does not divide \(n\) and consider the plane triangle (Newton polygon)
\[
\Delta_{n,q} := \{(j, i) \mid 0 \leq j, \quad 0 \leq i, \quad qj + ni \leq nq\}
\]
with the vertices \((0, 0), (0, q)\) and \((n, 0)\). Let \(L_{n,q}\) be the set of integer points in the interior of \(\Delta_{n,q}\). One may easily check that \(g = (q - 1)(n - 1)/2\) coincides with the number of elements of \(L_{n,q}\). It is also clear that for each \((j, i) \in L_{n,q}\)
\[
1 \leq j \leq n - 1; \quad 1 \leq i \leq q - 1; \quad q(j - 1) + (j + 1) \leq n(q - i).
\]
Elementary calculations ([2, theorem 3 on p. 403]) show that
\[ \omega_{j,i} := x^{j-1}dx/y^{q^i} = x^{j-1}y^i dx/y^{q^i} = x^{j-1}y^i dx/y^{q^i-1} \]
is a differential of the first kind on \( C \) for each \((j, i) \in L_{n,q}\). This implies easily that the collection \( \{\omega_{j,i}\}_{(j,i) \in L_{n,q}} \) is a basis in the space of differentials of the first kind on \( C \).

There is a non-trivial birational \( K_a \)-automorphism of \( C \)
\[ \delta_q : (x, y) \mapsto (x, \zeta y). \]
Clearly, \( \delta_q^q \) is the identity map and the set of fixed points of \( \delta_q \) coincides with \( B' \).

**Remark 4.3.** Let us assume that \( n = \deg(f) \) is divisible by \( q \) say, \( n = qm \) for some positive integer \( m \). Let \( \alpha \in K_a \) be a root of \( f \) and \( K_1 = K(\alpha) \) be the corresponding subfield of \( K_a \). We have \( f(x) = (x - \alpha)f_1(x) \) with \( f_1(x) \in K_1[x] \). Clearly, \( f_1(x) \) is a separable polynomial over \( K_1 \) of degree \( qm - 1 = n - 1 \geq 4 \). It is also clear that the polynomials
\[ h(x) = f_1(x + \alpha), h_1(x) = x^{n-1}h(1/x) \in K_1[x] \]
are separable of the same degree \( qm - 1 = n - 1 \geq 4 \). The standard substitution
\[ x_1 = 1/(x - \alpha), y_1 = y/(x - \alpha)^m \]
establishes a birational isomorphism between \( C_{f,p} \) and a curve
\[ C_{h_1} : y_1^q = h_1(x_1) \]
(see [14, p. 3359]). In particular, the jacobians of \( C_f \) and \( C_{h_1} \) are isomorphic over \( K_a \) (and even over \( K_1 \)). But \( \deg(h_1) = qm - 1 \) is not divisible by \( p \). Clearly, this isomorphism commutes with the actions of \( \delta_q \). Notice also that if the Galois group of \( f \) over \( K \) is \( S_n \) (resp. \( A_n \)) then the Galois group of \( h_1 \) over \( K_1 \) is \( SS_{n-1} \) (resp. \( A_{n-1} \)).

**Remark 4.4.**
(i) Let \( \Omega^1(C) = \Omega^1(C_{f,q}) \) be the \( K \)-vector space of differentials of the first kind on \( C \). It is well-known that \( \dim_K(\Omega^1(C_{f,q})) \) coincides with the genus of \( C_{f,q} \). By functoriality, \( \delta_q \) induces on \( \Omega^1(C_{f,q}) \) a certain \( K \)-linear automorphism
\[ \delta_q^*: \Omega^1(C_{f,q}) \to \Omega^1(C_{f,q}). \]
Clearly, if for some positive integer \( j \) the differential \( \omega_{j,i} = x^{j-1}dx/y^{q^{-i}} \) lies in \( \Omega^1(C_{f,q}) \) then it is an eigenvector of \( \delta_q^* \) with eigenvalue \( \zeta_i \).

(ii) Now assume that \( p \) does not divide \( n \). It follows from Remark 4.2 that the collection

\[
\{ \omega_{j,i} = x^{j-1}dx/y^{q^{-i}} \mid (i,j) \in L_{n,q} \}
\]

is an eigenbasis of \( \Omega^1(C_{f,q}) \). This implies that the multiplicity of the eigenvalue \( \zeta^{-i} \) of \( \delta_q^* \) coincides with number of interior integer points in \( \Delta_{n,q} \) along the corresponding (to \( q - i \)) horizontal line. Elementary calculations show that this number is \( \left\lfloor \frac{ni}{q} \right\rfloor \); in particular, \( \zeta^{-i} \) is an eigenvalue if and only if \( \left\lfloor \frac{ni}{q} \right\rfloor > 0 \).

It also follows easily that 1 is not an eigenvalue \( \delta_q^* \). This implies that

\[
\mathcal{P}_q(\delta_q^*) = \delta_q^{*q-1} + \cdots + \delta_q^* + 1 = 0
\]

in \( \text{End}_K(\Omega^1(C_{f,q})) \). In addition, one may easily check that if \( H(t) \) is a polynomial with rational coefficients such that \( H(\delta_q^*) = 0 \) in \( \text{End}_K(\Omega^1(C_{f,q})) \) then \( H(t) \) is divisible by \( \mathcal{P}_q(t) \) in \( \mathbb{Q}[t] \).

Let \( J(C_{f,q}) = J(C) = J(C_{f,q}) \) be the jacobian of \( C \). It is a \( g \)-dimensional abelian variety defined over \( K \) and one may view (via Albanese functoriality) \( \delta_q \) as an element of

\[
\text{Aut}(C) \subset \text{Aut}(J(C)) \subset \text{End}(J(C))
\]

such that \( \delta_q \neq \text{Id} \) but \( \delta_q^2 = \text{Id} \) where \( \text{Id} \) is the identity endomorphism of \( J(C) \). Here \( \text{Aut}(C) \) stands for the group of \( K_a \)-automorphisms of \( C \), \( \text{Aut}(J(C)) \) stands for the group of \( K_a \)-automorphisms of \( J(C) \) and \( \text{End}(J(C)) \) stands for the ring of all \( K_a \)-endomorphisms of \( J(C) \). We write \( \mathbb{Z}[\delta_q] \) for the subring of \( \text{End}(J(C)) \) generated by \( \delta_q \). As usual, we write \( \text{End}^0(J(C)) = \text{End}^0(J(C_{f,q})) \) for the corresponding \( \mathbb{Q} \)-algebra \( \text{End}(J(C)) \otimes \mathbb{Q} \). We write \( \mathbb{Q}[\delta_q] \) for the \( \mathbb{Q} \)-subalgebra of \( \text{End}^0(J(C)) \) generated by \( \delta_q \).

**Remark 4.5.** Assume that \( p \) does not divide \( n \). Let \( P_0 \) be one of the \( \delta_q \)-invariant points (i.e., a ramification point for \( \pi \)) of \( C_{f,p}(K_a) \). Then

\[
\tau : C_{f,q} \to J(C_{f,q}), \quad P \mapsto \text{cl}((P) - (P_0))
\]
is an embedding of complex algebraic varieties and it is well-known that the induced map

$$\tau^*: \Omega^1(J(C_{f,q})) \to \Omega^1(C_{f,q})$$

is a $C$-linear isomorphism obviously commuting with the actions of $\delta_q$. (Here $cl$ stands for the linear equivalence class.) This implies that $n_\sigma$ coincides with the dimension of the eigenspace of $\Omega^1(C_{f,q})$ attached to the eigenvalue $\zeta^{-i}$ of $\delta_q^*$. Applying Remark 4.4, we conclude that if $H(t)$ is a monic polynomial with integer coefficients such that $H(\delta_q) = 0$ in $\text{End}(J(C_{f,q}))$ then $H(t)$ is divisible by $P_q(t)$ in $\mathbb{Q}[t]$ and therefore in $\mathbb{Z}[t]$.

**Remark 4.6.** Assume that $p$ does not divide $n$. Clearly, the set $S$ of eigenvalues $\lambda$ of

$$\delta_q^*: \Omega^1(J(C_{f,q})) \to \Omega^1(J(C_{f,q}))$$

with $P_q/\lambda(\lambda) \neq 0$ consists of primitive $q$th roots of unity $\zeta^{-i}$ $(1 \leq i < q, (i,p) = 1)$ with $\left\lceil \frac{ni}{q} \right\rceil > 0$ and the multiplicity of $\zeta^{-i}$ equals $\left\lfloor \frac{ni}{q} \right\rfloor$, thanks to Remarks 4.5 and 4.4. Let us compute the sum

$$M = \sum_{1 \leq i < q, (i,p) = 1} \left\lfloor \frac{ni}{q} \right\rfloor$$

of multiplicities of eigenvalues from $S$.

First, assume that $q > 2$. Then $\varphi(q) = (p - 1)p^{r-1}$ is even and for each (index) $i$ the difference $q - i$ is also prime to $p$, lies between 1 and $q$ and

$$\left\lfloor \frac{ni}{q} \right\rfloor + \left\lfloor \frac{n(q-i)}{q} \right\rfloor = n - 1.$$

It follows easily that

$$M = (n - 1)\varphi(q) = \frac{(n - 1)(p - 1)p^{r-1}}{2}.$$

Now assume that $q = p = 2$ and therefore $r = 1$. Then $n$ is odd,

$$C_{f,q} = C_{f,2} : y^2 = f(x)$$

is a hyperelliptic curve of genus $g = \frac{n-1}{2}$ and

$$\delta_2 : (x,y) \mapsto (x,-y).$$

It is well-known that the differentials $x^i \frac{dx}{y}$ $(0 \leq i \leq g - 1)$ constitute a basis of the $g$-dimensional $\Omega^1(J(C_{f,2}))$. It follows that $\delta_2^*$ is just multiplication by $-1$. Therefore

$$M = g = \frac{n - 1}{2} = \frac{(n - 1)(p - 1)p^{r-1}}{2}.$$
Notice that if the abelian (sub)variety \( Z := \mathcal{P}_{q/p}(\delta_q)(J(C_{f,q})) \) has dimension \( M \) then the data \( Y = J(C_{f,q}), \delta = \delta_q, P = \mathcal{P}_{q/p}(t) \) satisfy the conditions of Theorem 3.9.

**Lemma 4.7.** Assume that \( p \) does not divide \( n \). Let \( D = \sum_{P \in B} a_P(P) \) be a divisor on \( C = C_{f,p} \) with degree 0 and support in \( B \). Then \( D \) is principal if and only if all the coefficients \( a_P \) are divisible by \( q \).

**Proof.** Suppose \( D = \text{div}(h) \) where \( h \in K_a(C) \) is a non-zero rational function of \( C \). Since \( D \) is \( \delta_q \)-invariant, the rational function \( \delta_q^* h := h \delta_q = c \cdot h \) for some non-zero \( c \in K_a \). It follows easily from the \( \delta_q \)-invariance of the splitting \( K_a(C) = \oplus_{i=0}^{q-1} y^i \cdot K_a(x) \) that

\[
\delta_q^* h := h \delta_q = c \cdot h
\]

for some non-zero \( c \in K_a \). It follows easily from the \( \delta_q \)-invariance of the splitting

\[
K_a(C) = \oplus_{i=0}^{q-1} y^i \cdot K_a(x)
\]

that

\[
h = y^i \cdot u(x)
\]

for some non-zero rational function \( u(x) \in K_a(x) \) and a non-negative integer \( i \leq q-1 \). It follows easily that all finite zeros and poles of \( u(x) \) lie in \( B \), i.e., there exists an integer-valued function \( b \) on \( \mathfrak{R}_f \) such that \( u \) coincides, up to multiplication by a non-zero constant, to \( \prod_{\alpha \in \mathfrak{R}_f} (x - \alpha)^{b(\alpha)} \). Notice that

\[
\text{div}(y) = \sum_{P \in B} (P) - n(\infty).
\]

On the other hand, for each \( \alpha \in \mathfrak{R}_f \), we have \( P_\alpha = (\alpha,0) \in B \) and the corresponding divisor

\[
\text{div}(x - \alpha) = q((\alpha,0)) - q(\infty) = q(P_\alpha) - q(\infty)
\]

is divisible by \( q \). This implies that

\[
a_{P_\alpha} = q \cdot b(\alpha) + i.
\]

Also, since \( \infty \) is neither zero no pole of \( h \),

\[
0 = ni + \sum_{\alpha \in \mathfrak{R}_f} b(\alpha)q.
\]

Since \( n \) and \( q \) are relatively prime, \( i \) must divide \( q \). This implies that \( i = 0 \) and therefore the divisor

\[
D = \text{div}(u(x)) = \text{div}(\prod_{\alpha \in \mathfrak{R}_f} (x - \alpha)^{b(\alpha)})
\]
is divisible by $q$.

Conversely, suppose a divisor $D = \sum_{P \in B} a_P(P)$ with $\sum_{P \in B} a_P = 0$ and all $a_P$ are divisible by $q$. Let us put
\[ h = \prod_{P \in B} (x - x(P))^{a_P/q}. \]
One may easily check that $D = \text{div}(h)$. \hfill \square

Lemma 4.8. $1 + \delta_q + \cdots + \delta_q^{q-1} = 0$ in $\text{End}(J(C_{f,q}))$. The subring $\mathbb{Z}[\delta_q] \subset \text{End}(J(C_{f,q}))$ is isomorphic to the ring $\mathbb{Z}[t]/\mathcal{P}_q(t)[t]$. The $\mathbb{Q}$-subalgebra $\mathbb{Q}[\delta_q] \subset \text{End}^0(J(C_{f,q})) = \text{End}^0(J(C_{f,q}))$ is isomorphic to $\mathbb{Q}[t]/\mathcal{P}_q(t)[t] = \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p_i})$.

Proof. If $q = p$ is a prime this assertion is proven in [9, p. 149], [10, p. 458]. So, further we may assume that $q > p$. It follows from Remark 4.3 that we may assume $p$ does not divide $n$.

Now we follow arguments of [10, p. 458] (where the case of $q = p$ was treated). The group $J(C_{f,q})(K_a)$ is generated by divisor classes of the form $(P) - (\infty)$, where $P$ is a finite point on $C_{f,p}$. The divisor of the rational function $x - x(P)$ is $(\delta_q^{q-1}P) + \cdots + (\delta_qP) + (P) - q(\infty)$. This implies that
\[ \mathcal{P}_q(\delta_q) = 0 \in \text{End}(J(C_{f,q})). \]
Applying Remark 4.5(ii), we conclude that $\mathcal{P}_q(t)$ is the minimal polynomial of $\delta_q$ in $\text{End}(J(C_{f,q}))$. \hfill \square

Let us define the abelian (sub)variety
\[ J^{(f,q)} := \mathcal{P}_{q/p}(\delta_q)(J(C_{f,q})) \subset J(C_{f,q}). \]
Clearly, $J^{(f,q)}$ is a $\delta_q$-invariant abelian subvariety defined over $K(\zeta_q)$. In addition,
\[ \Phi_q(\delta_q)(J^{(f,q)}) = 0. \]

Remark 4.9. If $q = p$ then $\mathcal{P}_{q/p}(t) = \mathcal{P}_1(t) = 1$ and therefore $J^{(f,p)} = J(C_{f,p})$.

Remark 4.10. Since the polynomials $\Phi_q$ and $\mathcal{P}_{q/p}$ are relatively prime, the homomorphism
\[ \mathcal{P}_{q/p}(\delta_q) : J^{(f,q)} \rightarrow J^{(f,q)} \]
has finite kernel and therefore is an isogeny. In particular, it is surjective.

Lemma 4.11. (i) If $p$ does not divide $n$ then $\dim(J^{(f,q)}) = (p^{r} - p^{r-1})/(n-1)$.
If $q$ divides $n$ then $\dim(J^{(f,q)}) = (p^{r} - p^{r-1})(n-2)/2$.
(ii) If $p$ does not divide $n$ then there is an $K(\zeta_q)$-isogeny $J(C_{f,q}) \to J(C_{f,q/p}) \times J^{(f,q)}$.

(iii) If $p$ does not divide $n$ and $\zeta \in K$ then the Galois modules $V_{f,p}$ and

$$(J^{(f,q)})^{(\delta_q)} := \{ z \in J^{(f,q)}(K_a) \mid \delta_q(z) = z \}$$

are isomorphic.

Proof. Clearly, we may assume that $\zeta \in K$. It follows from Remark 4.3 that we may assume that $p$ does not divide $n$. Clearly, the assertion (ii) implies the assertion (i). Further we will prove the assertions (ii) and (iii).

Let us consider the curve

$$C_{f,q/p} : y_1^{q/p} = f(x_1)$$

and a regular surjective map

$$\pi_1 : C_{f,q} \to C_{f,q/p}, \quad x_1 = x, y_1 = y^p.$$  

Clearly,

$$\pi_1 \delta_q = \delta_{q/p} \pi_1.$$

By Albanese functoriality, $\pi_1$ induces a certain surjective homomorphism of jacobians $J(C_{f,q}) \to J(C_{f,q/p})$ which we continue to denote by $\pi_1$. Clearly, the equality $\pi_1 \delta_q = \delta_{q/p} \pi_1$ remains true in $\text{Hom}(J(C_{f,q}), J(C_{f,q/p}))$. By Lemma 4.8

$$P_{q/p}(\delta_{q/p}) = 0 \in \text{End}(J(C_{f,q/p})).$$

It follows from Lemma 4.10 that

$$\pi_1(J^{(f,q)}) = 0.$$  

It follows that $\dim(J^{(f,q)})$ does not exceed

$$\dim(J(C_{f,q})) - \dim(J(C_{f,q/p})) = \frac{(p^r - 1)(n - 1)}{2} - \frac{(p^{r-1} - 1)(n - 1)}{2} = \frac{(p^r - p^{r-1})(n - 1)}{2}.$$  

By definition of $J^{(f,q)}$, for each divisor $D = \sum_{P \in B} a_P(P)$ the linear equivalence class of

$$p^{r-1}D = \sum_{P \in B} p^{r-1}a_P(P)$$

lies in $(J^{(f,q)})^{(\delta_q)} \subset J^{(f,q)}(K_a) \subset J(C_{f,q})(K_a)$. It follows from Lemma 4.17 that the class of $p^{r-1}D$ is zero if and only if all $p^{r-1}a_P$ are divisible by $q = p^r$, i.e. all $a_P$ are divisible by $p$. This implies that the set of linear equivalence classes of $p^{r-1}D$ is a Galois submodule isomorphic to $V_{f,p}$. We need to prove that $(J^{(f,q)})^{(\delta_q)} = V_{f,p}$.
Recall that $J^{(f,q)}$ is $\delta_p$-invariant and the restriction of $\delta_q$ to $J^{(f,q)}$ satisfies the $q$th cyclotomic polynomial. This allows us to define the homomorphism

$$\mathbb{Z}[\zeta_q] \to \text{End}(J^{(f,q)})$$

which sends 1 to the identity map and $\zeta_q$ to $\delta_q$. Let us put

$$E = \mathbb{Q}(\zeta_q) , \mathcal{O} = \mathbb{Z}[\zeta_q] \subset \mathbb{Q}(\zeta_q) = E.$$ 

It is well-known that $\mathcal{O}$ is the ring of integers in $E$, 

$$\lambda = (1 - \zeta_q)\mathbb{Z}[\zeta_q] = (1 - \zeta_q)\mathcal{O}$$

is a maximal ideal in $\mathcal{O}$ with $\mathcal{O}/\lambda = \mathbb{F}_p$ and $\mathcal{O} \otimes \mathbb{Z}_p = \mathbb{Z}_p[\zeta_q]$ is the ring of integers in the field $\mathbb{Q}_p(\zeta_q)$. Notice also that $\mathcal{O} \otimes \mathbb{Z}_p$ coincides with the completion $\mathcal{O}_\lambda$ of $\mathcal{O}$ with respect to $\lambda$-adic topology and $\mathcal{O}_\lambda/\lambda \mathcal{O}_\lambda = \mathcal{O}/\lambda = \mathbb{F}_p$.

It follows (see [7]) that

$$d = \frac{2\dim(J^{(f,q)})}{E : \mathbb{Q}} = \frac{2\dim(J^{(f,q)})}{p^r - p^{r-1}}$$

is a positive integer and the $\mathbb{Z}_p$-Tate module $T_p(J^{(f,q)})$ is a free $\mathcal{O}_\lambda$-module of rank $d$. It follows that $T_p(J^{(f,q)}) \otimes_{\mathcal{O}_\lambda} \mathbb{F}_p$ is a $d$-dimensional vector space. On the other hand, clearly

$$(J^{(f,q)})^{\delta_q} = \{ u \in J^{(f,q)}(K_a) \mid (1 - \delta_p)(u) = 0 \} = J^{(f,q)}_\lambda = T_p(J^{(f,q)}) \otimes_{\mathcal{O}_\lambda} \mathbb{F}_p.$$ 

Since $(J^{(f,q)})^{\delta_q}$ contains $(n-1)$-dimensional $\mathbb{F}_p$-vector space $V_{f,p}$,

$$d \geq n - 1.$$ 

This implies that

$$2\dim(J^{(f,q)}) = d(p^r - p^{r-1}) \geq (n-1)(p^r - p^{r-1})$$

and therefore

$$\dim(J^{(f,q)}) \geq \frac{(n-1)(p^r - p^{r-1})}{2}.$$ 

But we have already seen that

$$\dim(J^{(f,q)}) \leq \frac{(n-1)(p^r - p^{r-1})}{2}.$$ 

This implies that

$$\dim(J^{(f,q)}) = \frac{(n-1)(p^r - p^{r-1})}{2}.$$ 

It follows that $d = n - 1$ and therefore

$$(J^{(f,q)})^{\delta_q} = V_{f,p}.$$
Corollary 4.12. If \( p \) does not divide \( n \) then there is a \( K(\zeta_q) \)-isogeny \( J(C_{f,q}) \to J(C_{f,p}) \times \prod_{i=2}^{n^2} J(f,p^i) = \prod_{i=1}^{n^2} J(f,p^i) \).

Proof. Combine Corollary 4.11(ii) and Remark 4.9 with easy induction by \( r \). □

Remark 4.13. Suppose that \( p \) does not divide \( n \) and consider the induced linear operator

\[
\delta_q^*: \Omega^1(J(f,q)) \to \Omega^1(J(f,q)).
\]

It follows from Theorem 3.9 combined with Remark 4.6 that its spectrum consists of primitive \( q \)-th roots of unity \( \zeta^{-i} \) (\( 1 \leq i < q \)) with \( \left\lfloor \frac{ni}{q} \right\rfloor > 0 \) and the multiplicity of \( \zeta^{-i} \) equals \( \left\lfloor \frac{ni}{q} \right\rfloor \).

Theorem 4.14. Suppose that \( n \geq 5 \) is an integer. Let \( p \) be a prime, \( r \geq 1 \) an integer and \( q = p^r \). Suppose that \( p \) does not divide \( n \). Suppose that \( K \) is a field of characteristic different from \( p \) containing a primitive \( q \)-th root of unity \( \zeta \). Let \( f(x) \in K[x] \) be a separable polynomial of degree \( n \) and \( \text{Gal}(f) \) its Galois group. Suppose that the \( \text{Gal}(f) \)-module \( V_{f,p} \) is very simple. Then the image \( \mathcal{O} \) of

\[
\mathbb{Z}[\delta_q] \to \text{End}(J(f,q))
\]

is isomorphic to \( \mathbb{Z}[\zeta_q] \) and enjoys one of the following two properties.

(i) \( \mathcal{O} \) is a maximal commutative subring in \( \text{End}(J(f,q)) \);

(ii) \( \text{char}(K) > 0 \) and the centralizer of \( \mathcal{O} \otimes \mathbb{Q} \cong \mathbb{Q}(\zeta_q) \) in \( \text{End}^0(J(f,q)) \) is a central simple \( (n-1)^2 \)-dimensional \( \mathbb{Q}(\zeta_q) \)-algebra.

Proof. Clearly, \( \mathcal{O} \) is isomorphic to \( \mathbb{Z}[\zeta_q] \). Let us put \( \lambda = (1 - \zeta_q)\mathbb{Z}[\zeta_q] \). By Lemma 4.11(iii), the Galois module \( (J(f,q))^\delta_\lambda = J_{\lambda}^0(f,q) \) is isomorphic to \( V_{f,p} \). Applying Theorem 3.7 we conclude that either (ii) holds true or one of the following conditions hold:

(a) \( \mathcal{O} \) is a maximal commutative subring in \( \text{End}(J(f,q)) \);

(b) \( \text{char}(K) = 0 \) and there exist a \( \frac{\varphi(q)}{2} \)-dimensional abelian variety \( Z \) over \( K_a \), an embedding \( \mathbb{Q}(\zeta_q) \hookrightarrow \text{End}^0(Z) \) and a \( \mathbb{Q}(\zeta_q) \)-equivariant isogeny \( \psi : Z^{n-1} \to J(f,q) \).

Clearly, if (a) is fulfilled then we are done.

If \( q = p \) and \( \text{char}(K) = 0 \) then it is known [17], [19, Th. 5.3] that (a) is fulfilled.
So further we may assume that (b) holds true. In particular, \( \text{char}(K) = 0 \). We may also assume that \( q > p \). In order to finish the proof, we need to arrive to a contradiction. Clearly, \( \psi \) induces an isomorphism
\[
\psi^* : \Omega^1(J(f,q)) \cong \Omega^1(Z^{n-1})
\]
that commutes with the action of \( Q(\zeta_q) \). (Here again we use that \( \text{char}(K) = 0 \).)

Since \( \dim\Omega^1(Z) = \frac{\varphi(q)}{2} \), the linear operator in \( \Omega^1(Z) \) induced by \( \zeta_q \) has, at most, \( \frac{\varphi(q)}{2} \) distinct eigenvalues. It follows that the linear operator in \( \Omega^1(Z^{n-1}) = \Omega^1(Z)^{n-1} \) induced by \( \zeta_q \) also has, at most, \( \frac{\varphi(q)}{2} \) distinct eigenvalues. This implies that the linear operator \( \delta_q^* \) in \( \Omega^1((J(f,q))) \) also has, at most, \( \frac{\varphi(q)}{2} \) distinct eigenvalues. Recall that the eigenvalues of \( \delta_q^* \) are primitive \( q \)-th roots of unity \( \zeta^{-i} \) with
\[
1 \leq i < q, (i, p) = 1, \left\lfloor \frac{ni}{q} \right\rfloor > 0.
\]
Clearly, the inequality \( \left\lfloor \frac{ni}{q} \right\rfloor > 0 \) means that \( ni \geq q \), i.e.
\[
i \geq \frac{q}{n} \geq \frac{q}{5}.
\]
So, in order to get a desired contradiction, it suffices that the cardinality of the set of integers
\[
B := \left\{ i \mid \frac{q}{5} \leq i < q = p^r, (i, p) = 1 \right\}
\]
is strictly greater than \( (p - 1)p^{r-1}/2 \). Indeed, clearly, \( \frac{q}{5} < \frac{p^{r-1}}{2} \) and
\[
\#(B) > \varphi(q) - \frac{q}{5} = (p - 1)p^{r-1} - \frac{p^{r-1}p}{5} = (p - 1 - \frac{p}{5})p^{r-1} > \frac{p - 1}{2}p^{r-1}.
\]

\( \square \)

**Corollary 4.15.** Suppose that \( n \geq 5 \) is an integer. Let \( p \) be a prime, \( r \geq 1 \) an integer and \( q = p^r \). Assume in addition that either \( p \) does not divide \( n \) or \( q \mid n \) and \( (n, q) \neq (5, 5) \). Let \( K \) be a field of characteristic different from \( p \), Let \( f(x) \in K[x] \) be an irreducible separable polynomial of degree \( n \) such that \( \text{Gal}(f) = S_n \) or \( A_n \). Then the image \( \mathcal{O} \) of
\[
\mathbb{Z}[\delta_q] \to \text{End}(J(f,q))
\]
is isomorphic to \( \mathbb{Z}[\zeta_q] \) and enjoys one of the following two properties.

- (i) \( \mathcal{O} \) is a maximal commutative subring in \( \text{End}(J(f,q)) \);
Remark 2.1 allows us to do it, using the action of $J$ on differentials of the first kind on $\Omega$. Let $\Sigma = \Sigma_1$ be the set of all field embeddings $\sigma : E = \mathbb{Q}[\delta_q] \hookrightarrow \mathbb{C}$. We are going to apply Theorem 2.2 to $Z = J^{[f]}$ and $E = \mathbb{Q}[\delta_q]$. In order to do that we need to get some information about the multiplicities

$$n_\sigma = n_\sigma(Z, E) = n_\sigma(J^{[f]}, \mathbb{Q}[\delta_q]).$$

Remark 2.1 allows us to do it, using the action of $\mathbb{Q}[\delta_q]$ on the space $\Omega_1(J^{[f]})$ of differentials of the first kind on $J^{[f]}$.

In other words, $\Omega_1(J^{[f]})_\sigma$ is the eigenspace corresponding to the eigenvalue $\sigma(\delta_q)$ of $\delta_q$ and $n_\sigma$ is the multiplicity of the eigenvalue $\sigma(\delta_q)$.

Let $i < q$ be a positive integer that is not divisible by $p$ and $\sigma_i : \mathbb{Q}[\delta_p] \hookrightarrow \mathbb{C}$ be the embedding which sends $\delta_p$ to $\zeta^{-i}$. Clearly, for each $\sigma$ there exists precisely one $i$ such that $\sigma = \sigma_i$. Clearly, $\Omega_1(J^{[f]})$ is the eigenspace of $\Omega_1(J^{[f]})$ attached to the eigenvalue $\zeta^{-i}$ of $\delta_q$. Therefore $n_{\sigma_i}$ coincides with the multiplicity of the eigenvalue $\zeta^{-i}$. It follows from Remark 4.13 that

$$n_{\sigma_i} = \left\lfloor \frac{ni}{q} \right\rfloor.$$
Combining Corollary 4.15 and 4.16 we obtain the following statement.

**Theorem 4.17.** Let $p$ be a prime, $r$ a positive integer, $q = p^r$ and $K$ a field of characteristic zero. Suppose that $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\text{Gal}(f) = S_n$ or $A_n$. Assume also that either $p$ does not divide $n$ or $q$ divides $n$. Then $\text{End}^0(J^{f,q}) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}(\zeta_q)$ and therefore $\text{End}(J^{f,q}) = \mathbb{Z}[\delta_q] \cong \mathbb{Z}[\zeta_q]$. In particular, $J^{f,q}$ is an absolutely simple abelian variety.

Combining Theorem 4.16 and Corollary 4.14 we obtain the following statement.

**Theorem 4.18.** Let $p$ be a prime, $r$ a positive integer, $q = p^r$ and $K$ a field of characteristic zero. Let $f(x) \in K[x]$ be an irreducible polynomial of degree $n \geq 5$. Assume also that $p$ does not divide $n$ and the $\text{Gal}(f)$-module $V_{f,p}$ is very simple. Then $\text{End}^0(J^{f,q}) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}(\zeta_q)$ and therefore $\text{End}(J^{f,q}) = \mathbb{Z}[\delta_q] \cong \mathbb{Z}[\zeta_q]$. In particular, $J^{f,q}$ is an absolutely simple abelian variety.

5. Jacobians and their endomorphism rings

Throughout this section we assume that $K$ is a field of characteristic zero. Recall that $K_a$ is an algebraic closure of $K$ and $\zeta \in K_a$ is a primitive $q$th root of unity. Suppose $f(x) \in K[x]$ is a polynomial of degree $n \geq 5$ without multiple roots, $\mathfrak{R}_f \subset K_a$ is the set of its roots, $K(\mathfrak{R}_f)$ is its splitting field. Let us put

$$\text{Gal}(f) = \text{Gal}(K(\mathfrak{R}_f)/K) \subset \text{Perm}(\mathfrak{R}_f).$$

Let $r$ be a positive integer. Recall (Corollary 4.12) that if $p$ does not divide $n$ then there is a $K(\zeta_{q^r})$-isogeny $J(C_{f,p^r}) \to \prod_{i=1}^r J^{f,q^i}$. Applying Theorem 4.18 to all $q = p^i$, we obtain the following assertions.

**Theorem 5.1.** Let $p$ be a prime, $r$ a positive integer, $q = p^r$ and $K$ a field of characteristic zero. Let $f(x) \in K[x]$ be an irreducible polynomial of degree $n \geq 5$. Assume also that $p$ does not divide $n$ and the $\text{Gal}(f)$-module $V_{f,p}$ is very simple. Then

$$\text{End}^0(J(C_{f,q})) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}[t]/\mathbb{Q}(\zeta_q) \cong \prod_{i=1}^r \mathbb{Q}(\zeta_{q^i}).$$

**Theorem 5.2.** Let $p$ be a prime, $r$ a positive integer and $K$ a field of characteristic zero. Suppose that $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\text{Gal}(f) = S_n$ or $A_n$. Assume also that either $p$ does not divide $n$ or

$$\text{End}^0(J(C_{f,q})) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}[t]/\mathbb{Q}(\zeta_q) \cong \prod_{i=1}^r \mathbb{Q}(\zeta_{q^i}).$$
Proof. The existence of the isogeny $J(C_{f,q}) \rightarrow \prod_{i=1}^{r} J^{f(p^i)}$ combined with Theorem 4.17 implies that the assertion holds true if $p$ does not divide $n$. If $q$ divides $n$ then Remark 4.3 allows us to reduce this case to the already proven case when $p$ does not divide $n − 1$. □

Example 5.3. Suppose $L = \mathbb{C}(z_1, \cdots, z_n)$ is the field of rational functions in $n$ independent variables $z_1, \cdots, z_n$ with constant field $\mathbb{C}$ and $K = L^S_n$ is the subfield of symmetric functions. Then $K_a = L_a$ and

$$f(x) = \prod_{i=1}^{n} (x - z_i) \in K[x]$$

is an irreducible polynomial over $K$ with Galois group $S_n$. Let $q = p^r$ be a power of a prime $p$. Let $C$ be a smooth projective model of the $K$-curve $y^q = f(x)$ and $J(C)$ its jacobian. It follows from Theorem 5.2 that if $n \geq 5$ and either $p$ does not divide $n$ or $q$ divides $n$ then the algebra of $L_a$-endomorphisms of $J(C)$ is $\prod_{i=1}^{r} Q(\zeta_{p^i})$.

Example 5.4. Let $h(x) \in \mathbb{C}[x]$ be a Morse polynomial of degree $n \geq 5$. This means that the derivative $h'(x)$ of $h(x)$ has $n − 1$ distinct roots $\beta_1, \cdots, \beta_{n−1}$ and $h(\beta_i) \neq h(\beta_j)$ while $i \neq j$. (For example, $x^n - x$ is a Morse polynomial.) Let $K = \mathbb{C}(z)$ be the field of rational functions in variable $z$ with constant field $\mathbb{C}$ and $K_a$ its algebraic closure. Then a theorem of Hilbert ([13, theorem 4.4.5, p. 41]) asserts that the Galois group of $h(x) − z$ over $k(z)$ is $S_n$. Let $q = p^r$ be a power of a prime $p$. Let $C$ be a smooth projective model of the $K$-curve $y^q = h(x) − z$ and $J(C)$ its jacobian. It follows from Theorem 5.2 that if either $p$ does not divide $n$ or $q$ divides $n$ then the algebra of $K_a$-endomorphisms of $J(C)$ is $\prod_{i=1}^{r} Q(\zeta_{p^i})$.

References

[1] I. N. Herstein, Noncommutative rings. John Wiley and Sons, 1968.
[2] J. K. Koo, On holomorphic differentials of some algebraic function field of one variable over $\mathbb{C}$. Bull. Austral. Math. Soc. 43 (1991), 399–405.
[3] S. Lang, Abelian varieties, Springer Verlag 1983.
[4] B. Moonen and Yu. G. Zarhin, Weil classes on abelian varieties. J. reine angew. Math. 496 (1998), 83–92.
[5] B. Mortimer, The modular permutation representations of the known doubly transitive groups. Proc. London Math. Soc. (3) 41 (1980), 1–20.
[6] D. Mumford, Abelian varieties, 2nd edn (Oxford University Press, 1974).
[7] K. Ribet, Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. 98 (1976), 751–804.
K. Ribet, *Hodge classes on certain abelian varieties*. Amer. J. Math. **105** (1983), 523–538.

B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*. J. reine angew. Math. **488** (1997), 141–188.

E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*. Math. Ann. **310** (1998), 447–471.

I. Schur, *Gleichungen ohne Affect*. Sitz. Preuss. Akad. Wiss. 1930, Physik-Math. Klasse 443–449 (=Ges. Abh. III, 191–197).

J.-P. Serre, Abelian ℓ-adic representations and elliptic curves. AK Peters, Wellesley, 1998.

J.-P. Serre, *Topics in Galois Theory*. Jones and Bartlett Publishers, 1992.

C. Towse, *Weierstrass points on cyclic covers of the projective line*. Trans. Amer. Math. Soc. **348** (1996), 3355–3377.

Yu. G. Zarhin, *Weights of simple Lie algebras in the cohomology of algebraic varieties*. Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), 264–304; English translation: Math. USSR Izv. **24** (1985), 245 - 281.

Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.

Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (eds. C. Faber, G. van der Geer and F. Oort). Progress in Math., vol. **195** (Birkhäuser, 2001), pp. 473–490.

Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication in positive characteristic*. Math. Res. Letters **8** (2001), 429–435.

Yu. G. Zarhin, *Cyclic covers of the projective line, their jacobians and endomorphisms*. J. reine angew. Math. **544** (2002), 91–110.

Yu. G. Zarhin, *Endomorphism rings of certain jacobians in finite characteristic*. Matem. Sbornik **193** (2002), issue 8, 39–48; Sbornik Math., 2002, **193** (8), 1139-1149.

Yu. G. Zarhin, *Very simple 2-adic representations and hyperelliptic jacobians*. Moscow Math. J. **2** (2002), issue 2, 403-431.

Yu. G. Zarhin, *Homomorphisms of hyperelliptic jacobians*. In: Number Theory, Algebra, and Algebraic geometry (Shafarevich Festschrift), Proc. Steklov Math. Institute **241** (2003), 90–104; e-print: [http://arXiv.org/abs/math.NT/0301173](http://arXiv.org/abs/math.NT/0301173).

Yu. G. Zarhin, *The endomorphism rings of jacobians of cyclic covers of the projective line*. Math. Proc. Cambridge Philos. Soc. **136** (2004), to appear.

Yu. G. Zarhin, *Very simple representations: variations on a theme of Clifford*. In: Galois Theory Conference Proceedings (H. Völklein, ed.), Developments in Math., Kluwer, to appear; e-print: [http://front.math.ucdavis.edu/math.GR/0209083](http://front.math.ucdavis.edu/math.GR/0209083).

Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians*. e-print: [http://front.math.ucdavis.edu/math.AG/0311137](http://front.math.ucdavis.edu/math.AG/0311137).

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

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