THE ENDOMORPHISM RINGS OF JACOBIANS OF CYCLIC
COVERS OF THE PROJECTIVE LINE

BY YURI G. ZARHIN †

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

e-mail: zarhin@math.psu.edu

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 $p$ be an odd prime, $\mathbb{Z}[\zeta_p]$ the ring of integers in the
$p$th cyclotomic field $\mathbb{Q}(\zeta_p)$. Suppose $C$ is the smooth projective model of the
affine curve $y^p = f(x)$ and $J(C)$ is the jacobian of $C$. We prove that the ring
$\text{End}(J(C))$ of $K_a$-endomorphisms of $J(C)$ is canonically isomorphic to $\mathbb{Z}[\zeta_p]$.

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 an
odd prime, $\zeta_p \in \mathbb{C}$ a primitive $p$th root of unity, $\mathbb{Q}(\zeta_p) \subset \mathbb{C}$ the $p$th cyclotomic field
and $\mathbb{Z}[\zeta_p]$ the ring of integers in $\mathbb{Q}(\zeta_p)$. It is well-known that $\mathbb{Q}(\zeta_p)$ is a CM-field
of degree $p - 1$. We write $\mathbb{F}_p$ for the finite field consisting of $p$ elements.

Let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 4$ without multiple roots. Let
$C_{f,p}$ be a smooth projective model of the smooth affine curve

$$y^p = f(x).$$

It is well-known that the genus $g(C_{f,p})$ of $C_{f,p}$ is $(p - 1)(n - 1)/2$ if $p$ does not
divide $n$ and $(p - 1)(n - 2)/2$ if it does. The map

$$(x, y) \mapsto (x, \zeta_p y)$$

† Partially supported by the NSF.
Yuri G. Zarhin

gives rise to a non-trivial birational automorphism

\[ \delta_p : C_{f,p} \to C_{f,p} \]
of period \( p \).

The jacobian \( J^{(f,p)} := J(C_{f,p}) \) of \( C_{f,p} \) is an abelian variety of dimension \( g(C_{f,p}) \). We write \( \text{End}(J^{(f,p)}) \) for the ring of endomorphisms of \( J^{(f,p)} \) over \( \mathbb{C} \). By Albanese functoriality, \( \delta_p \) induces an automorphism of \( J^{(f,p)} \) which we still denote by \( \delta_p \); it is known (\cite{10}, p. 149), \( \cite{11}, \text{p. 458} \) that

\[ \delta_p^{-1} + \cdots + \delta_p + 1 = 0 \]
in \( \text{End}(J^{(f,p)}) \). This gives us an embedding

\[ \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[\delta_p] \subset \text{End}(J^{(f,p)}) \]
(\cite{10}, p. 149), \( \cite{11}, \text{p. 458} \).

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 \( A_n \). Then

\[ \text{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p] \cong \mathbb{Z}[\zeta_p] . \]

In particular, \( J^{(f,p)} \) is a simple complex abelian variety.

**Remark 1.2.** In the case when \( p \) is a Fermat prime the assertion of Theorem 1.1 is proven in \( \cite{20} \). (Also in \( \cite{20} \) the author proved that if the conditions of Theorem 1.1 hold true then \( \mathbb{Z}[\delta_p] \) is a maximal commutative subring in \( \text{End}(J^{(f,p)}) \) for all odd primes \( p \). See \( \cite{21} \) for a similar result in positive characteristic when \( p \mid n \) and \( n \geq 9 \).) The “opposite” case when \( J^{(f,p)} \) is an abelian variety of CM-type was studied in \( \cite{2} \). An analogue of Theorem 1.1 for hyperelliptic jacobians (i.e., the case of \( p = 2 \)) was proven in \( \cite{17} \) (see also \( \cite{18}, \cite{19} \)).

**Examples 1.3.**

1. the polynomial \( x^n - x - 1 \in \mathbb{Q}[x] \) has Galois group \( S_n \) over \( \mathbb{Q} \) (\cite{13}, p. 42). Therefore the endomorphism ring (over \( \mathbb{C} \)) of the jacobian \( J(C) \) of the curve \( C : y^p = x^n - x - 1 \) is \( \mathbb{Z}[\zeta_p] \) if \( n \geq 5 \).

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 $A_n$. Therefore the endomorphism ring (over $C$) of the jacobian $J(C)$ of the curve $C : yp = \exp_n(x)$ is $Z[\zeta_p]$ if $n \geq 5$.

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

The paper is organized as follows. Section 3 contains auxiliary results about endomorphism algebras of complex abelian varieties. We use them in Section 4 in order to study endomorphisms of $J^{(f,p)}$. In Section 4 we prove the main result. The short last Section contains corrigendum to [20].

The author would like to thank the referee for useful comments.

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 $Q$-algebra $\text{End}(Z) \otimes Q$. 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 $H_1(Z, Q)$ be the first rational homology group of $Z$; it is a $2\dim(Z)$-dimensional $Q$-vector space. By functoriality $\text{End}^0(Z)$ acts on $H_1(Z, Q)$; hence we have an embedding

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

(which sends 1 to 1).

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

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

We write

$$\text{Tr}_E : \text{End}_E(H_1(Z, Q)) \to E$$

for the corresponding trace map on the $E$-algebra of $E$-linear operators in $H_1(Z, Q)$. 
Extending by $\mathbb{C}$-linearity the action of $\text{End}^0(Z)$ and of $E$ on the complex cohomology group

$$H_1(Z, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = H_1(Z, \mathbb{C})$$

of $Z$ we get the embeddings

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

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

$$E_{\mathbb{C}} = E \otimes_{\mathbb{Q}} \mathbb{C} = \prod_{\sigma \in \Sigma_E} E \otimes_{E, \sigma} \mathbb{C} = \prod_{\sigma \in \Sigma_E} C_{\sigma}$$

where

$$C_{\sigma} = E \otimes_{E, \sigma} \mathbb{C} = \mathbb{C}.$$

Since $H_1(Z, \mathbb{C})$ is a free $E_{\mathbb{C}}$-module of rank $d$, there is the corresponding trace map

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

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

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

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

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

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

We write $\sigma' : E \hookrightarrow \mathbb{C}$ for the composition of $\sigma : E \hookrightarrow \mathbb{C}$ and the complex conjugation $\mathbb{C} \to \mathbb{C}$. The embedding $\sigma' \in \Sigma_E$ is (called) the complex-conjugate of $\sigma$.

**Remark 2.1.** It is well-known ([1], p. 53), ([3], p. 84)] that

$$n_{\sigma} + n_{\sigma'} = d \quad \forall \sigma \in \Sigma_E.$$
Remark 2.2. 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 $E \otimes \overline{\mathbb{C}}$-module in such a way that

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

In particular,

$$n_\sigma = \dim_C(\text{Lie}(Z) \sigma) = \dim_C(\Omega^1(Z) \sigma).$$

Theorem 2.3. Suppose $E$ contains $\mathfrak{C}_Z$. Then the tuple

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

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

Proof. The inclusion $\mathfrak{C}_Z \subset E$ implies that $\mathfrak{C}_Z$ is a field.

There is a canonical Hodge decomposition ([7, chapter 1], [1, pp. 52–53])

$$H^1(Z, \mathbb{C}) = H^{-1,0} \oplus H^{0,-1}$$

where $H^{-1,0}$ and $H^{0,-1}$ are mutually “complex conjugate” $\dim(Z)$-dimensional complex vector spaces. This splitting is $\text{End}^0(Z)$-invariant and the $\text{End}^0(Z)$-module $H^{-1,0}$ is canonically isomorphic to $\text{Lie}(Z)$. Let

$$f_H : H^1(Z, \mathbb{C}) \to H^1(Z, \mathbb{C})$$

be the $\mathbb{C}$-linear operator in $H^1(Z, \mathbb{C})$ defined as follows.

$$f_H(x) = -x \quad \forall x \in H^{-1,0}; \quad f_H(x) = 0 \quad \forall x \in H^{0,-1}.$$ 

Clearly, $f_H$ commutes with $\text{End}^0(Z)$ and therefore with $E$. Hence $f_H$ may be viewed as an endomorphism of the free $E \mathbb{C}$-module $H^1(Z, \mathbb{C})$; clearly, its trace is the tuple

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

Suppose $MT = MT_Z \subset \text{GL}_\mathbb{Q}(H^1(Z, \mathbb{Q}))$ is the Mumford-Tate group of (the rational Hodge structure $H^1(Z, \mathbb{Q})$ and of) $Z$ ([6, 9, 16]). It is a connected reductive
algebraic \( \mathbb{Q} \)-group that contains scalars and could be described as follows ([16, section 6.3]). Let \( m_t \subset \text{End}_{\mathbb{Q}}(H_1(Z, \mathbb{Q})) \) be the \( \mathbb{Q} \)-Lie algebra of \( MT \); it is a reductive algebraic linear \( \mathbb{Q} \)-Lie algebra which contains scalars and its natural faithful representation in \( H_1(Z, \mathbb{Q}) \) is completely reducible. In addition, \( m_t \) is the smallest \( \mathbb{Q} \)-Lie subalgebra in \( \text{End}_{\mathbb{Q}}(H_1(Z, \mathbb{Q})) \) enjoying the following property: its complexification

\[
m_t \mathbb{C} = m_t \otimes \mathbb{Q} \mathbb{C} \subset \text{End}_{\mathbb{C}}(H_1(Z, \mathbb{C}))
\]

contains scalars and \( f_H \). It is well-known that the centralizer of \( MT \) (and therefore of \( m_t \)) in \( \text{End}_{\mathbb{Q}}(H_1(Z, \mathbb{Q})) \) coincides with \( \text{End}^0(Z) \). This implies that the center \( \mathfrak{c} \) of \( m_t \) lies in \( \mathfrak{C}_Z \). Since \( m_t \) is reductive, it splits into a direct sum

\[
m_t = m_{t^{ss}} \oplus \mathfrak{c}
\]

of \( \mathfrak{c} \) and a semisimple \( \mathbb{Q} \)-Lie algebra \( m_{t^{ss}} \). Clearly, \( m_t \) lies in \( \text{End}_E(H_1(Z, \mathbb{Q})) \).

Since \( m_{t^{ss}} \) is semisimple and the trace map \( \text{Tr}_E \) is a Lie algebra homomorphism, \( \text{Tr}_E(m_{t^{ss}}) = \{0\} \). Since \( \mathfrak{c} \subset \mathfrak{C}_Z \subset E \), we have \( \text{Tr}_E(\mathfrak{c}) \subset \mathfrak{C}_Z \) and therefore

\[
\text{Tr}_E(m_t) \subset \mathfrak{C}_Z.
\]

This implies easily that

\[
\text{Tr}_{E_{\mathfrak{C}}}(m_t \mathbb{C}) \subset \mathfrak{C}_Z \otimes \mathbb{Q} \mathbb{C}.
\]

In particular, since \( f_H \in m_t \mathbb{C} \), we have \( \text{Tr}_{E_{\mathfrak{C}}}(f_H) \in \mathfrak{C}_Z \otimes \mathbb{Q} \mathbb{C} \). But \( \text{Tr}_{E_{\mathfrak{C}}}(f_H) = (-n_\sigma)_{\sigma \in \Sigma} \). This implies easily that

\[
(n_\sigma)_{\sigma \in \Sigma E} = -\text{Tr}_{E_{\mathfrak{C}}}(f_H) \in \mathfrak{C}_Z \otimes \mathbb{Q} \mathbb{C}.
\]

In order to prove the second assertion of the theorem, notice that its assumptions imply that \( E/\mathfrak{C}_Z \) is a nontrivial Galois extension. If \( \kappa : E \to E \) is a non-identity element of the Galois group \( \text{Gal}(E/\mathfrak{C}_Z) \) then one may easily check that

\[
\mathfrak{C}_Z \otimes \mathbb{Q} \mathbb{C} \subset \{(u)_{\sigma \in \Sigma E} \in \prod_{\sigma \in \Sigma E} \mathbb{C} = E_{\mathfrak{C}} \mid u_\sigma = u_{\sigma \kappa} \quad \forall \sigma\}.
\]

3. CYCLIC COVERS AND JACOBIANS

Throughout this paper we fix an odd prime \( p \) and assume that \( K \) is a field of characteristic zero. 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 \( p \)th root of unity \( \zeta \).
Let \( f(x) \in K[x] \) be a separable polynomial of degree \( n \geq 4 \). We write \( \mathcal{R}_f \) for the set of its roots and denote by \( L = L_f = K(\mathcal{R}_f) \subset K_n \) 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 \( \mathcal{R}_f \) and the natural map of \( \text{Gal}(f) \) into the group \( \text{Perm}(\mathcal{R}_f) \) of all permutations of \( \mathcal{R}_f \) is an embedding. We will identify \( \text{Gal}(f) \) with its image and consider it as a permutation group of \( \mathcal{R}_f \).

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

We refer the reader to [6, 20, 3, 8] for the definition and properties of the heart \( (F_{\mathcal{R}_f}^{\mathcal{R}_f})^{00} \) over the field \( F_p \) of the group \( \text{Gal}(f) \) acting on the set \( \mathcal{R}_f \). Here we just recall that \( (F_{\mathcal{R}_f}^{\mathcal{R}_f})^{00} \) is a finite-dimensional \( F_p \)-vector space provided with a natural structure of \( \text{Gal}(f) \)-module.

Let \( C = C_{f,p} \) be the smooth projective model of the smooth affine \( K \)-curve \( y^p = f(x) \).

So \( C \) is a smooth projective curve defined over \( K \). The rational function \( x \in K(C) \) defines a finite cover \( \pi : C \to \mathbf{P}^1 \) of degree \( p \). Let \( B' \subset C(K_n) \) be the set of ramification points. Clearly, the restriction of \( \pi \) to \( B' \) is an injective map \( B' \hookrightarrow \mathbf{P}^1(K_n) \), whose image is the disjoint union of \( \infty \) and \( \mathcal{R}_f \) if \( p \) does not divide \( \text{deg}(f) \) and just \( \mathcal{R}_f \) if it does. We write \( B = \pi^{-1}(\mathcal{R}_f) = \{ (\alpha, 0) \mid \alpha \in \mathcal{R}_f \} \subset B' \subset C(K_n) \).

Clearly, \( \pi \) is ramified at each point of \( B \) with ramification index \( p \). 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 \( p \). Using Hurwitz’s formula, one may easily compute the genus \( g = g(C) = g(C_{p,f}) \) of \( C \) ([8, pp. 401–402], [14, proposition 1 on p. 3359], [10, p. 148]). Namely, \( g \) is \( (p-1)(n-1)/2 \) if \( p \) does not divide \( n \) and \( (p-1)(n-2)/2 \) if it does.

**Remark 3.1.** Assume that \( p \) does not divide \( n \) and consider the plane triangle (Newton polygon)

\[
\Delta_{n,p} := \{ (j,i) \mid 0 \leq j, \ 0 \leq i, \ pj + ni \leq np \}
\]

with the vertices \((0,0), (0,p)\) and \((n,0)\). Let \( L_{n,p} \) be the set of integer points in the interior of \( \Delta_{n,p} \). One may easily check that \( g \) coincides with the number of
elements of $L_{n,p}$. It is also clear that for each $(j, i) \in L_{n,p}$
\[1 \leq j \leq n - 1; \quad 1 \leq i \leq p - 1; \quad p(j - 1) + (j + 1) \leq n(p - i).\]
Elementary calculations ([4, theorem 3 on p. 403]) show that
\[\omega_{j,i} := x^j-1 dx/y^i = x^j-1 y^i dx/y^p = x^j-1 y^{i-1} dx/y^{p-1}\]
is a differential of the first kind on $C$ for each $(j, i) \in L_{n,p}$. This implies easily that
the collection \{\omega_{j,i}\} $(j,i) \in L_{n,p}$ is a basis in the space of differentials of the first kind on $C$.

There is a non-trivial birational $K_a$-automorphism of $C$
\[\delta_p : (x, y) \mapsto (x, \zeta y).\]
Clearly, $\delta_p^p$ is the identity map and the set of fixed points of $\delta_p$ coincides with $B'$.
Let $J^{(f,p)} = J(C) = J(C_{f,p})$ be the jacobian of $C$. It is a $g$-dimensional abelian
variety defined over $K$ and one may view (via Albanese functoriality) $\delta_p$ as an element of
\[\text{Aut}(C) \subset \text{Aut}(J(C)) \subset \text{End}(J(C))\]
such that $\delta_p \neq \text{Id}$ but $\delta_p^p = \text{Id}$ 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 $J(C)$. As usual, we write $\text{End}^0(J(C)) = \text{End}^0(J^{(f,p)})$ for the corresponding $Q$-algebra $\text{End}(J(C)) \otimes Q$.

**Lemma 3.2.** $\text{Id} + \delta_p + \cdots + \delta_p^{p-1} = 0$ in $\text{End}(J(C))$. Therefore the subring $\mathbb{Z}[\delta_p] \subset \text{End}(J(C))$ is isomorphic to the ring $\mathbb{Z}[\zeta_p]$ of integers in the $p$th cyclotomic field $Q(\zeta_p)$. The $Q$-subalgebra $Q[\delta_p] \subset \text{End}^0(J(C)) = \text{End}^0(J^{(f,p)})$ is isomorphic to $Q(\zeta_p)$.

**Proof.** See [14, p. 149], [11, p. 458].

**Remark 3.3.** If $K$ contains $\zeta$ then the Galois modules $(F_{p^m})^{00}$ and $\ker(\text{Id} - \delta_p)$
are canonically isomorphic ([14, proposition 6.2], [11, proposition 3.2]).

**Remark 3.4.** Recall that $p$ is odd and assume that $n = \deg(f)$ is divisible by $p$
say, $n = pm$ for some positive integer $m$. Since $n \geq 4$, we conclude that $n \geq 5$.
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 $pm - 1 = n - 1 \geq 4$. 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 $pm - 1 = n - 1 \geq 4$. The standard substitution

$$x_1 = 1/(x - \alpha), y_1 = y/(x - \alpha)^n$$

establishes a birational isomorphism between $C_{f,p}$ and a curve

$$C_{h_1} : y_1^p = h_1(x_1)$$

(see [14, p. 3359]). But $\deg(h_1) = pm - 1$ is not divisible by $p$. Clearly, this isomorphism commutes with the actions of $\delta_p$.

**Theorem 3.5.** Suppose $n \geq 4$. Assume that $Q[\delta_p]$ is a maximal commutative subalgebra in $\text{End}^0(J^{(f,p)})$. Then the center $C$ of $\text{End}^0(J^{(f,p)})$ is a CM-subfield of $Q[\delta_p]$.

**Proof.** This is theorem 3.8 of [20].

**Theorem 3.6.** Suppose $n \geq 4$. Assume that $Q[\delta_p]$ is a maximal commutative subalgebra in $\text{End}^0(J^{(f,p)})$. Then $\text{End}^0(J^{(f,p)}) = Q[\delta_p] \cong Q(\zeta_p)$ and therefore $\text{End}(J^{(f,p)}) = Z[\delta_p] \cong Z[\zeta_p]$.

**Proof.** Let $\mathfrak{c} = \mathfrak{c}_{f,p}$ be the center of $\text{End}^0(J^{(f,p)})$. We know that $\mathfrak{c}$ is a CM-subfield of $E := Q[\delta_p]$.

Replacing, if necessary, $K$ by its subfield (finitely) generated over $Q$ by all the coefficients of $f$, we may assume that $K$ (and therefore $K_a$) is isomorphic to a subfield of the field $C$ of complex numbers. So, $K \subset K_a \subset C$. We may also assume that $\zeta = \zeta_p$ and consider $C_{f,p}$ as complex projective curve and its jacobian $J^{(f,p)}$ as complex abelian variety.

Let $\Sigma = \Sigma_E$ be the set of all field embeddings $\sigma : E = Q[\delta_p] \hookrightarrow C$. We are going to apply Theorem 2.3 to $Z = J^{(f,p)}$ and $E = Q[\delta_p]$. In order to do that we need to get some information about the multiplicities

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

Remark 2.2 allows us to do it, using the action of $Q[\delta_p]$ on the space $\Omega^1(J^{(f,p)})$ of differentials of the first kind on $J^{(f,p)}$. 
Recall that if $\sigma' : Q[\delta_p] \hookrightarrow C$ is the embedding complex conjugate to $\sigma$ then, by Remark 2.1,

$$n_\sigma + n_{\sigma'} = \frac{2\dim(J(f,p))}{p - 1},$$

since $[Q[\delta_p] : Q] = p - 1$. Notice also that for each $\sigma : Q[\delta_p] \hookrightarrow C$

$$\Omega^1(J(f,p))_\sigma = \{ \omega \in \Omega^1(J(f,p)) \mid \delta_p(\omega) = \sigma(\delta_p)\omega \}.$$ 

In other words, $\Omega^1(J(f,p))_\sigma$ is the eigenspace corresponding to the eigenvalue $\sigma(\delta_p)$ of $\delta_p$ and $n_\sigma$ is the multiplicity of the eigenvalue $\sigma(\delta_p)$.

Let $i < p$ be a positive integer and $\sigma_i : Q[\delta_p] \hookrightarrow C$ be the embedding which sends $\delta_p$ to $\zeta^{-i}$. Obviously, the complex conjugate of $\sigma_i$ coincides with $\sigma_{p-i}$. In addition, for each $\sigma$ there exists precisely one $i$ such that $\sigma = \sigma_i$. Clearly, $\Omega^1(J(f,p))_\sigma_i$ is the eigenspace of $\Omega^1(J(f,p))$ attached to the eigenvalue $\zeta^{-i}$ of $\delta_p$. Therefore $n_{\sigma_i}$ coincides with the multiplicity of the eigenvalue $\zeta^{-i}$.

Let $P_0$ be one of the $\delta_p$-invariant points (i.e., a ramification point for $\pi$) of $C_{f,p}(K_\lambda) \subset C_{f,p}(C)$. Then

$$\tau : C_{f,p} \to J(f,p), \quad P \mapsto \text{cl}((P) - (P_0))$$

is an embedding of complex algebraic varieties and it is well-known that the induced map

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

is a $C$-linear isomorphism obviously commuting with the actions of $\delta_p$. (Here $\text{cl}$ stands for the linear equivalence class.) This implies that $n_{\sigma_i}$ coincides with the dimension of the eigenspace of $\Omega^1(C_{f,p})_p$ attached to the eigenvalue $\zeta^{-i}$ of $\delta_p$.

**Remark 3.7.** Clearly, if for some positive integer $j$ the differential $x^{i-1}dx/y^{p-i}$ lies in $\Omega^1(C_{f,p})$ then it is an eigenvector of $\delta_p$ with eigenvalue $\zeta^i$. Now assume that $p$ does not divide $n$. It follows from Remark 2.1 that each $n_\sigma = n_{\sigma_i}$ could be visualized as the number of interior integer points in $\Delta_{n,p}$ along the corresponding (to $p - i$) horizontal line. Elementary calculations show that this number is $\lfloor \frac{ni}{p} \rfloor$. This implies that $n_{\sigma_i} = \lfloor \frac{ni}{p} \rfloor$ for $1 \leq i \leq p - 1$. Then $n_{\sigma_i} = 0$ if and only if $1 \leq i \leq \lfloor \frac{p}{n} \rfloor$.

Assume, in addition, that $p < n$. Clearly, in this case the function $i \mapsto n_{\sigma_i} = \lfloor \frac{ni}{p} \rfloor$ is strictly increasing.

**Remark 3.8.** Assume that $p$ divides $n$. Then $n \geq 5$ and $n - 1 \geq 4$. Clearly, $p$ does not divide $n - 1$. Applying Remark 3.4, we get a curve $C_{h_{1,p}} : y_1^p = h_1(x_1)$
with separable polynomial $h_1(x_1)$ of degree $n - 1$ and a $\delta_p$-equivariant birational isomorphism between $C_{f,p}$ and $C_{h_1,p}$. This gives us a $\delta_p$-equivariant isomorphism

$$\Omega^1(C_{f,p}) \cong \Omega^1(C_{h_1,p}).$$

Applying Remark 3.7 to $C_{h_1,p}$ and $n - 1$ (instead of $C_{f,p}$ and $n$), we conclude that $n_{\sigma_i} = \lfloor \frac{(n-1)i}{p} \rfloor$ for $1 \leq i \leq p - 1$. Then $n_{\sigma_i} = 0$ if and only if $1 \leq i \leq \lfloor \frac{p}{n-1} \rfloor$.

Assume, in addition, that $n \neq p$. Clearly, in this case $n - 1 > p$ and the function $i \mapsto n_{\sigma_i} = \lfloor \frac{(n-1)i}{p} \rfloor$ is strictly increasing.

**Proposition 3.9.**

(i) let us assume that $p > n$. Then $n_{\sigma} = 0$ if and only if $\sigma = \sigma_i$ with $1 \leq i \leq \lfloor \frac{p-1}{n} \rfloor$.

(ii) let us assume that $p = n$. Then $n_{\sigma} = 0$ if and only if $\sigma = \sigma_i$ with $i = 1$.

**Proof of Proposition 3.9.** First, assume that $p > n$. Clearly, $p$ does not divide $n$ and therefore $\lfloor \frac{p}{n} \rfloor = \lfloor \frac{p-1}{n} \rfloor$. Now the assertion (i) follows from Remark 3.7.

Now assume that $p = n$. By Remark 3.8, $n_{\sigma_i} = 0$ if and only if $1 \leq i \leq \lfloor \frac{p}{n-1} \rfloor$. But $\lfloor \frac{p}{n-1} \rfloor = \lfloor \frac{p}{p-1} \rfloor = 1$.

**Proposition 3.10.** Let us assume that $p < n$. If $\sigma, \iota$ are two embeddings $Q[\delta_p] \hookrightarrow C$ then $n_{\sigma} = n_{\iota}$ if and only if $\sigma = \iota$.

**Proof of Proposition 3.10.** First assume that $p$ does not divide $n$. Then the assertion follows from (the last sentence of) Remark 3.7.

Now assume that $p$ divides $n$. Then the assertion follows from (the last sentence of) Remark 3.8.

**End of the proof of Theorem 3.6.** If $C = Q[\delta_p]$ then we are done, since $Q[\delta_p]$ is a maximal commutative subalgebra in $\text{End}^0(J^{(f,p)})$. Assume that $C \neq Q[\delta_p]$. Our goal is to get a contradiction.

Clearly, $Q[\delta_p]/Q$ is a Galois extension. It follows from Theorem 2.3 and Remark 2.2 (applied to $Z = J^{(f,p)}$ and $E = Q[\delta_p]$) that there exists a non-trivial field automorphism $\kappa : Q[\delta_p] \to Q[\delta_p]$ such that for all $\sigma \in \Sigma$

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

Clearly, there exists an integer $m$ such that $1 < m < p$ and $\kappa(\delta_p) = \delta_p^m$.

First, assume that $n > p$. It follows from Proposition 3.10 that $\sigma\kappa = \sigma$ which could not be the case, since $\kappa$ is not the identity map. This contradiction proves the Theorem in the case of $n > p$. 


Second, assume that $n = p$. It follows from Proposition 3.9(ii) that $\sigma_1 \kappa = \sigma_1$ which, by the same token, leads to a contradiction.

Third, assume that $p > n$. It follows from Proposition 3.9(i) that the map $\sigma \mapsto \sigma \kappa$ permutes the set $\{\sigma_i \mid 1 \leq i \leq \left\lfloor \frac{(p-1)n}{n} \right\rfloor\}$. Since $\kappa(\delta_p) = \delta_p^m$, $\sigma_i \kappa(\delta_p) = \zeta^{-im}$. This implies that multiplication by $m$ in $\mathbb{F}_p^*$ leaves invariant the subset $A := \{i \mod p \in \mathbb{F}_p \mid 1 \leq i \leq \left\lfloor \frac{(p-1)n}{n} \right\rfloor\}$. This implies that $m = m \cdot 1 \leq \left\lfloor \frac{(p-1)n}{n} \right\rfloor = \frac{(p-1)}{4}$.

Let us consider the arithmetic progression consisting of the $m$ integers $\left\lfloor \frac{(p-1)n}{n} \right\rfloor + 1, \ldots, \left\lfloor \frac{(p-1)n}{n} \right\rfloor + m$ with difference 1. All its elements lie between $\left\lfloor \frac{(p-1)n}{n} \right\rfloor + 1$ and $\left\lfloor \frac{(p-1)n}{n} \right\rfloor + m \leq \frac{2(p-1)}{2} = p - 1$.

Clearly, there exists a positive integer $r \leq m$ such that $\left\lfloor \frac{(p-1)n}{n} \right\rfloor + r$ is divisible by $m$, i.e., there is a positive integer $d$ such that $md = \left\lfloor \frac{(p-1)n}{n} \right\rfloor + r$. Since $\left\lfloor \frac{(p-1)n}{n} \right\rfloor \geq m \geq 2$, we have $d \leq \left\lfloor \frac{(p-1)n}{n} \right\rfloor$ but $md = \left\lfloor \frac{(p-1)n}{n} \right\rfloor + r \leq \left\lfloor \frac{(p-1)n}{n} \right\rfloor + m < p - 1$. This implies that $A$ is not invariant under multiplication by $m$ which gives the desired contradiction.

4. Jacobians and their endomorphism rings

Recall that $K$ is a field of characteristic zero, $K_a$ is its algebraic closure. Suppose $f(x) \in K[x]$ is a polynomial of degree $n \geq 5$ without multiple roots, $\mathcal{R}_f \subset K_a$ is the set of its roots, $K(\mathcal{R}_f)$ is its splitting field. Let us put

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

**Theorem 4.1** (corollary 5.3 of [20]). Let $p$ be an odd prime. If $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\text{Gal}(f) = S_n$ or $A_n$ then $\mathbb{Q}[\delta_p]$ is a maximal commutative subalgebra in $\text{End}^0(J^{(f,p)})$ and the center of $\text{End}^0(J^{(f,p)})$ is a CM-subfield of $\mathbb{Q}[\delta_p]$.

Combining Theorems 4.1 and 3.6 we obtain the following statement.

**Theorem 4.2.** Let $p$ be an odd prime. If $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\text{Gal}(f) = S_n$ or $A_n$ then $\text{End}^0(J^{(f,p)}) = \mathbb{Q}[\delta_p]$ and therefore $\text{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p] \cong \mathbb{Z}[\zeta_p]$.

Clearly, Theorem 1.1 is a special case of Theorem 4.2.
Example 4.3. 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 $C$ be a smooth projective model of the $K$-curve $y^p = f(x)$ and $J(C)$ its jacobian. It follows from Theorem 4.2 that if $n \geq 5$ then the ring of $L_a$-endomorphisms of $J(C)$ is $\mathbb{Z}[\zeta_p]$. In particular, the abelian variety $J(C)$ is absolutely simple. When $p = 3$ and $3 \mid n$ the absolute simplicity of $J(C)$ was proven in ([15, p. 107]).

Example 4.4. 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 ([15, theorem 4.4.5, p. 41]) asserts that the Galois group of $h(x) - z$ over $k(z)$ is $S_n$. Let $C$ be a smooth projective model of the $K$-curve $y^p = h(x) - z$ and $J(C)$ its jacobian. It follows from Theorem 4.2 that the ring of $K_a$-endomorphisms of $J(C)$ is $\mathbb{Z}[\zeta_p]$. In particular, the abelian variety $J(C)$ is absolutely simple.

We refer the reader to [18, 19, 20, 22] for the definition and basic properties of very simple representations.

Theorem 4.5. Suppose $p$ is an odd prime, $n \geq 5$ and $K$ contains a primitive $p$th root of unity. If the Gal($f$)-module $(\mathbb{F}_p^{nr})^{00}$ is very simple then $\mathbb{Q}[\delta_p]$ coincides with its own centralizer in $\text{End}^0(J(f,p))$.

Proof. See theorem 5.2 of [20].

Theorem 4.6. Suppose $p$ is an odd prime, $n \geq 5$ and $K$ contains a primitive $p$th root of unity. If the Gal($f$)-module $(\mathbb{F}_p^{nr})^{00}$ is very simple then $\text{End}^0(J(f,p)) = \mathbb{Q}[\delta_p]$ and therefore $\text{End}(J(f,p)) = \mathbb{Z}[\delta_p] \cong \mathbb{Z}[\zeta_p]$.

Proof. It is an immediate corollary of Theorem [20] combined with Theorem 3.6.

5. Corrigendum to [20]

Remark 2.1 on p. 94, the last assertion. In general, it is not necessarily true that $G$ is doubly transitive ([3, Beispiel 2c], [18]). However, it becomes true if one
assumes additionally that either $p$ does not divide $n$ or $G$ is transitive and $p$ is an odd number dividing $n$ ([$3$, Satz 4a and Satz 11], [$20$, lemma 2.4]).

Lemma 2.4 on p. 95. Its assertion is essentially contained in Satz 4a of [$3$].

Remark 2.5 on p. 95. Its assertion is essentially Hilfssatz 3b of [$3$].

Sections 1, 3 and 5. Everywhere $\mathbb{Q}(\delta_p)$ means $\mathbb{Q}[\delta_p]$. (However, it does not make a difference, since $\mathbb{Q}[\delta_p]$ is a field.)

References

[1] P. Deligne, Hodge cycles on abelian varieties (notes by J.S. Milne). Lecture Notes in Math., vol. 900 (Springer-Verlag, 1982), pp. 9–100.

[2] J. de Jong and R. Noot, Jacobians with complex multiplications. In: *Arithmetic algebraic geometry* (eds. G. van der Geer, F. Oort and J. Steenbrink). Progress in Math., vol. 89 (Birkhäuser, 1991), pp. 177–192.

[3] M. Klemm, Über die Reduktion von Permutationsmoduln. *Math. Z.* 143 (1975), 113–117.

[4] 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.

[5] B. Moonen and Yu. G. Zarhin, Weil classes on abelian varieties. *J. reine angew. Math.* 496 (1998), 83–92.

[6] B. Mortimer, The modular permutation representations of the known doubly transitive groups. *Proc. London Math. Soc.* (3) 41 (1980), 1–20.

[7] D. Mumford, *Abelian varieties*, 2nd edn (Oxford University Press, 1974).

[8] P. M. Neumann, Review of [$3$], MR 52 #544.

[9] K. Ribet, Hodge classes on certain abelian varieties. *Amer. J. Math.* 105 (1983), 523–538.

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

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

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

[13] J.-P. Serre, *Topics in Galois Theory* (Jones and Bartlett Publishers, 1992).

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

[15] H. Völklein, Cyclic covers of $\mathbb{P}^1$ and Galois actions on their division points. *Contemporary Math.* 186 (1994), 91–107.

[16] 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.

[17] Yu. G. Zarhin, Hyperelliptic Jacobians without complex multiplication. *Math. Res. Letters* 7 (2000), 123–132.
[18] 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.

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

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

[21] Yu. G. Zarhin, Endomorphism rings of certain jacobians in finite characteristic. *Matem. Sbornik* 193 (2002), issue 8 (Russian), to appear.

[22] Yu. G. Zarhin, Very simple 2-adic representations and hyperelliptic jacobians; available at http://arXiv.org/abs/math.AG/0109014. *Moscow Math. J.* 2 (2002), issue 2, to appear.