ENDOMORPHISM ALGEBRAS OF SUPERELLIPTIC JACOBIANS

YURI G. ZARHIN

1. Introduction

As usual, we write $\mathbf{Z}, \mathbf{Q}, \mathbf{F}_p, \mathbf{C}$ for the ring of integers, the field of rational numbers, the finite field with p elements and the field of complex numbers respectively. If Z is a smooth algebraic variety over an algebraically closed field then we write $\Omega^1(Z)$ for the space of differentials of the first kind on Z. If Z is an abelian variety then we write $\mathrm{End}(Z)$ for its ring of (absolute) endomorphisms and $\mathrm{End}^0(Z)$ for its endomorphism algebra $\mathrm{End}(Z) \otimes \mathbf{Q}$. If Z is defined over a (not necessarily algebraically closed) field K then we write $\mathrm{End}_K(Z) \subset \mathrm{End}(Z)$ for the (sub)ring of K-endomorphisms of Z.

Let p be a prime, $q = p^r$ an integral power of p, $\zeta_q \in \mathbf{C}$ a primitive qth root of unity, $\mathbf{Q}(\zeta_q) \subset \mathbf{C}$ the qth cyclotomic field and $\mathbf{Z}[\zeta_q]$ the ring of integers in $\mathbf{Q}(\zeta_q)$. If $q = 2$ then $\mathbf{Q}(\zeta_q) = \mathbf{Q}$. It is well-known that if $q > 2$ then $\mathbf{Q}(\zeta_q)$ is a CM-field of degree $(p-1)p^{r-1}$. Let us put

$$\mathcal{P}_q(t) = \frac{t^q - 1}{t - 1} = t^{q-1} + \cdots + 1 \in \mathbf{Z}[t].$$

Clearly, $\mathcal{P}_q(t) = \prod_{i=1}^r \Phi_{p^i}(t)$ where $\Phi_{p^i}(t) = t^{(p-1)p^{i-1}} + \cdots + t^{p^{i-1}} + 1 \in \mathbf{Z}[t]$ is the p^ith cyclotomic polynomial. In particular, $\mathbf{Q}[t]/\Phi_{p^i}(t)\mathbf{Q}[t] = \mathbf{Q}(\zeta_{p^i})$ and $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

Let $f(x) \in \mathbf{C}[x]$ 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 $y^q = f(x)$. 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 a complex abelian variety. By Albanese functoriality, δ_q induces an automorphism of $J(C_{f,q})$ which we still denote by δ_q. One may easily check (see 4.8 below) that $\delta_q^{q-1} + \cdots + \delta_q + 1 = 0$ in $\mathrm{End}(J(C_{f,q}))$. This implies that if $\mathbf{Q}[\delta_q]$ is the $\mathbf{Q}$-subalgebra of $\mathrm{End}^0(J(C_{f,q}))$ generated by δ_q then there is the natural surjective homomorphism $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] \twoheadrightarrow \mathbf{Q}[\delta_q]$ that sends $t + \mathcal{P}_q(t)\mathbf{Q}[t]$ to δ_q. One may check that this homomorphism is, in fact, an isomorphism (see [7, p. 149], [8, p. 458]) where the case $q=p$ was treated). This gives us an embedding $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] \cong \mathbf{Q}[\delta_q] \subset \mathrm{End}^0(J(C_{f,q}))$. Our main result is the following statement.

Theorem 1.1. *Let K be a subfield of $\mathbf{C}$ such that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \ge 5$ and its Galois group over K is either the full symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. In addition, assume that either p does not divide n or $q \mid n$. Then $\mathrm{End}^0(J(C_{f,q})) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^{r} \mathbf{Q}(\zeta_{p^i})$.*

Remark 1.2. If q is a prime (i.e. $q=p$) then $J(C_{f,p})$ is an absolutely simple abelian variety and $\mathrm{End}(J(C_{f,p})) = \mathbf{Z}[\delta_p] \cong \mathbf{Z}[\zeta_p]$ [14, 20]. In particular, if $p=2$ then $C_{f,2}$ is a hyperelliptic curve, δ_2 is multiplication by -1 and $\mathrm{End}(J(C_{f,2})) = \mathbf{Z}$. See [19, 22, 18] for a discussion of finite characteristic case.

Examples 1.3. Let $n \ge 5$ be an integer, p a prime, r a positive integer, $q=p^r$. Assume also that either n is not divisible by p or $q \mid n$.

(1) The polynomial $x^n - x - 1 \in \mathbf{Q}[x]$ has Galois group $\mathbf{S}_n$ over $\mathbf{Q}$ ([11, p. 42]). Therefore the endomorphism algebra (over $\mathbf{C}$) of the jacobian $J(C)$ of the curve $C: y^q = x^n - x - 1$ is $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t]$.

(2) The Galois group of the "truncated exponential"
$$\exp_n(x) := 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!} \in \mathbf{Q}[x]$$
is either $\mathbf{S}_n$ or $\mathbf{A}_n$ [9]. Therefore the endomorphism algebra (over $\mathbf{C}$) of the jacobian $J(C)$ of the curve $C: y^q = \exp_n(x)$ is $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t]$.

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 $K_a \subset \mathbf{C}$ 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 $\mathbf{Q}[\delta_q]$ coincides with the $\mathbf{Q}$-algebra of K_a-endomorphisms of $J(C_{f,q})$.

Our main technical tool used in the proof of Theorem 1.1 is a certain modular representation $V_{f,p}$ of the Galois group of f [3, 17] arising from its action on the roots of f. In the case of $q=p$ the Galois module $V_{f,p}$ is canonically isomorphic to the subgroup of δ_p-invariants in $J(C_{f,p})$ (if $\zeta_p \in K$) [7, 8]. In the present paper we construct (assuming that $\zeta_q \in K$ and p does not divide n) an abelian subvariety $J^{f,q} \subset J(C_{f,q})$ with multiplication by $\mathbf{Z}[\zeta_q]$ and prove that $V_{f,p}$ is canonically isomorphic to the subgroup of ζ_q-invariants in $J^{f,q}$ (Lemma 4.11). (It turns out that if $q = p^r$ then $J(C_{f,q})$ is isogenous to a product of all J^{f,p^i} with $1 \le i \le r$.)

The paper is organized as follows. In §2 we obtain conditions that guarantee that the center of the endomorphism algebra of a complex abelian variety is a cyclotomic field (Corollary 2.2). In §3 we study abelian varieties X over arbitrary fields, whose endomorphism ring contains a subring isomorphic to the ring $\mathcal{O}$ of integers in a given number field E. We study the Galois action on the λ-torsion X_λ of X where λ is a maximal ideal in $\mathcal{O}$. We prove (Theorem 3.8) that if the Galois module X_λ is *very simple* in the sense of [15, 21] then the centralizer of E in the algebra $\mathrm{End}^0(X)$ of all (absolute) endomorphisms of X either coincides with E or is "very big". In §4 we study endomorphism algebras of $J^{(f,q)}$, using the very simplicity of the Galois module $V_{f,p}$ when $\deg(f) \ge 5$ and the Galois group of f is either the full symmetric or the alternating group. Theorem 3.8 helps us to prove that in characteristic zero $\mathbf{Q}(\zeta_q)$ is a maximal commutative subalgebra in $\mathrm{End}^0(J^{f,q})$. Using Corollary 2.2 and computations with differentials of the first kind (Theorem 3.10 and Remark 4.2), we prove (Theorem 4.16) that the center of $\mathrm{End}^0(J^{f,q})$ coincides with $\mathbf{Q}(\zeta_q)$ and therefore $\mathrm{End}^0(J^{f,q}) = \mathbf{Q}(\zeta_q)$. We finish the proof of Theorem 1.1 in §5.

2. Complex abelian varieties

Let Z be a complex abelian variety of positive dimension. We write $\mathfrak{C}_Z$ for the center of the semisimple finite-dimensional $\mathbf{Q}$-algebra $\mathrm{End}^0(Z)$.

Let E be a subfield of $\mathrm{End}^0(Z)$ that contains the identity map. Let Σ_E be the set of all field embeddings $\sigma : E \hookrightarrow \mathbf{C}$. It is well-known that

$$\mathbf{C}_\sigma := E \otimes_{E,\sigma} \mathbf{C} = \mathbf{C}, \quad E_{\mathbf{C}} = E \otimes_{\mathbf{Q}} \mathbf{C} = \prod_{\sigma \in \Sigma_E} E \otimes_{E,\sigma} \mathbf{C} = \prod_{\sigma \in \Sigma_E} \mathbf{C}_\sigma.$$

Let $\mathrm{Lie}(Z)$ be the tangent space to the origin of Z; it is a $\dim(Z)$-dimensional $\mathbf{C}$-vector space. By functoriality, $\mathrm{End}^0(Z)$ and therefore E act on $\mathrm{Lie}(Z)$ and therefore provide $\mathrm{Lie}(Z)$ with a natural structure of $E \otimes_{\mathbf{Q}} \mathbf{C}$-module. Clearly,

$$\mathrm{Lie}(Z) = \bigoplus_{\sigma \in \Sigma_E} \mathbf{C}_\sigma \mathrm{Lie}(Z) = \oplus_{\sigma \in \Sigma_E} \mathrm{Lie}(Z)_\sigma$$

where $\mathrm{Lie}(Z)_\sigma := \mathbf{C}_\sigma \mathrm{Lie}(Z) = \{x \in \mathrm{Lie}(Z) \mid ex = \sigma(e)x \quad \forall e \in E\}$. Let us put $n_\sigma = n_\sigma(Z,E) = \dim_{\mathbf{C}_\sigma} \mathrm{Lie}(Z)_\sigma = \dim_{\mathbf{C}} \mathrm{Lie}(Z)_\sigma$. It is well-known that the natural map $\Omega^1(Z) \to \mathrm{Hom}_{\mathbf{C}}(\mathrm{Lie}(Z), \mathbf{C})$ is an isomorphism. This allows us to define via duality the natural homomorphism $E \to \mathrm{End}_{\mathbf{C}}(\mathrm{Hom}_{\mathbf{C}}(\mathrm{Lie}(Z), \mathbf{C})) =$

$\mathrm{End}_{\mathbf{C}}(\Omega^1(Z))$. This provides $\Omega^1(Z)$ with a natural structure of $E\otimes_{\mathbf{Q}}\mathbf{C}$-module in such a way that $\Omega^1(Z)_\sigma := \mathbf{C}_\sigma\Omega^1(Z) \cong \mathrm{Hom}_{\mathbf{C}}(\mathrm{Lie}(Z)_\sigma, \mathbf{C})$. In particular,

$$n_\sigma = \dim_{\mathbf{C}}(\mathrm{Lie}(Z)_\sigma) = \dim_{\mathbf{C}}(\Omega^1(Z)_\sigma) \qquad (1).$$

The following statement is contained in [20, Th. 2.3].

Theorem 2.1. *If $E/\mathbf{Q}$ is Galois, E contains $\mathfrak{C}_Z$ and $\mathfrak{C}_Z \ne E$ then there exists a nontrivial automorphism $\kappa: E \to E$ such that $n_\sigma = n_{\sigma\kappa}$ for all $\sigma \in \Sigma_E$.*

The following assertion will be used in the proof of Theorem 4.16.

Corollary 2.2. *Suppose that there exist a prime p, a positive integer r, the prime power $q = p^r$ and an integer $n \ge 4$ enjoying the following properties:*

(i) *$E = \mathbf{Q}(\zeta_q) \subset \mathbf{C}$ where $\zeta_q \in \mathbf{C}$ is a primitive qth 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 $\sigma_i : E = \mathbf{Q}(\zeta_q) \hookrightarrow \mathbf{C}$ the embedding that sends ζ_q to ζ_q^{-i}. Then $n_{\sigma_i} = \left[\frac{ni}{q}\right]$.*

Then $\mathfrak{C}_Z = \mathbf{Q}(\zeta_q)$.

Proof. If $q = 2$ then $E = \mathbf{Q}(\zeta_2) = \mathbf{Q}$. Since $\mathfrak{C}_Z$ is a subfield of $E = \mathbf{Q}$, we conclude that $\mathfrak{C}_Z = \mathbf{Q} = \mathbf{Q}(\zeta_2)$. So, further we assume that $q > 2$.

Clearly, $\{\sigma_i\}$ is the collection Σ of all embeddings $\mathbf{Q}(\zeta_q) \hookrightarrow \mathbf{C}$. By (iii), $n_{\sigma_i} = 0$ if and only if $1 \le i \le [\frac{q}{n}]$. Suppose that $\mathfrak{C}_Z \ne \mathbf{Q}(\zeta_q)$. It follows from Theorem 2.1 that there exists a non-trivial field automorphism $\kappa : \mathbf{Q}[\zeta_q] \to \mathbf{Q}[\zeta_q]$ such that for all $\sigma \in \Sigma$ we have $n_\sigma = n_{\sigma\kappa}$. 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 $i \mapsto n_{\sigma_i} = [\frac{ni}{q}]$ is strictly increasing and therefore $n_{\sigma_i} \ne n_{\sigma_j}$ while $i \ne j$. This implies that $\sigma_i = \sigma_i\kappa$, i.e. κ is the identity map which is not the case. The obtained contradiction implies that $n < q$. Since $n \ge 4$, we have $q \ge 5$.

If i is an integer then we write $\bar{i} \in \mathbf{Z}/q\mathbf{Z}$ for its residue modulo q.

Clearly, $n_\sigma = 0$ if and only if $\sigma = \sigma_i$ with $1 \le i \le [\frac{q}{n}]$. Since n and q are relatively prime, $[\frac{q}{n}] = [\frac{q-1}{n}]$. It follows that $n_{\sigma_i} = 0$ if and only if $1 \le i \le [\frac{q-1}{n}]$. Clearly, the map $\sigma \mapsto \sigma\kappa$ permutes the set

$$\{\sigma_i \mid 1 \le i \le \left[\frac{q-1}{n}\right], p \text{ does not divide } i\}.$$

Since $\kappa(\zeta_q)=\zeta_q^m$ and $\sigma_i\kappa(\zeta_q)=\zeta_q^{-im}$, it follows that if

$$A:=\left\{i\in \mathbf{Z}\mid 1\le i\le \left[\frac{q-1}{n}\right]<q,\ p \text{ does not divide } i\right\}$$

then the multiplication by m in $(\mathbf{Z}/q\mathbf{Z})^*=\mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q})$ leaves invariant the set $\bar{A}:=\{\bar{i}\in \mathbf{Z}/q\mathbf{Z}\mid i\in A\}$. Clearly, A contains 1 and therefore $\bar{m}=m\cdot\bar{1}\in\bar{A}$. Since $1<m<q$,

$$m=m\cdot 1\le\left[\frac{q-1}{n}\right] \qquad (2).$$

Let us consider the arithmetic progression consisting of $2m$ integers

$$[\frac{q-1}{n}]+1,\dots,[\frac{q-1}{n}]+2m$$

with difference 1. All its elements lie between $[\frac{q-1}{n}]+1$ and

$$\left[\frac{q-1}{n}\right]+2m\le 3\left[\frac{q-1}{n}\right]\le 3\frac{q-1}{4}<q-1.$$

Clearly, there exist exactly two elements of A say, mc_1 and mc_1+m that are divisible by m. Clearly, c_1 is a positive integer and 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

$$\left[\frac{q-1}{n}\right]<mc\le\left[\frac{q-1}{n}\right]+2m<q-1 \qquad (3).$$

It follows that mc does not lie in A and therefore $\overline{mc}$ does not lie in $\bar{A}$. This implies that $\bar{c}$ also does not lie in $\bar{A}$ and therefore $c>\left[\frac{q-1}{n}\right]$. Using (3), we conclude that

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

and therefore

$$\left[\frac{q-1}{n}\right]<\frac{2m}{m-1}=2+\frac{2}{m-1}.$$

If $m>2$ then $m\ge 3$ and using (2), we conclude that

$$3\le m\le\left[\frac{q-1}{n}\right]<2+\frac{2}{m-1}\le 3$$

and therefore $3<3$, which is not true. Hence $m=2$ and

$$2=m\le\left[\frac{q-1}{n}\right]<2+\frac{2}{m-1}=4$$

and therefore $\left[\frac{q-1}{n}\right]=2$ or 3. It follows that $q\ge 1+2n\ge 1+2\cdot 4=9$. Since $m=2$ is not divisible by p, we conclude that $p\ge 3$ and either $\bar{A}=\{\bar{1},\bar{2}\}$ or $p>3$ and $A=\{\bar{1},\bar{2},\bar{3}\}$. In both cases $\bar{4}=2\cdot\bar{2}=m\cdot\bar{2}$ must lie in $\bar{A}$. Contradiction. □

3. Abelian varieties over arbitrary fields

Let K be a field. Let us fix its algebraic closure K_a and denote by $\mathrm{Gal}(K)$ the absolute Galois group $\mathrm{Aut}(K_a/K)$ of K. If X is an abelian variety of positive dimension over K_a then we write 1_X (or even just 1) for the identity automorphism of X. If Y is (may be another) abelian variety of positive dimension over K_a then we write $\mathrm{Hom}(X,Y)$ for the group of all K_a-homomorphisms from X to Y. We write $\mathrm{Hom}^0(X,Y)$ for the finite-dimensional $\mathbf{Q}$-vector space $\mathrm{Hom}(X,Y)\otimes\mathbf{Q}$. Clearly, $\mathrm{End}(X) = \mathrm{Hom}(X,X)$ and $\mathrm{End}^0(X) = \mathrm{End}(X)\otimes\mathbf{Q} = \mathrm{Hom}^0(X,X)$. It is well-known that $\mathrm{End}^0(X)$ is a finite-dimensional semisimple $\mathbf{Q}$-algebra and $\dim_{\mathbf{Q}}(\mathrm{End}^0(X))$ does not exceed $4\mathrm{dim}(X)^2$ [4, §19, corollary 1 to theorem 3]; the equality holds if and only if $\mathrm{char}(K)>0$ and X is a supersingular abelian variety [14, Lemma 3.1].

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_a and an embedding

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

with $i(1)=1_X$. It is well known [12, Proposition 2 on p. 36] that $[E:\mathbf{Q}]$ divides $2\mathrm{dim}(X)$, i.e., $r=r_X := 2\mathrm{dim}(X)/E:\mathbf{Q}]$ is a positive integer.

Let us denote by $\mathrm{End}^0(X,i)$ the centralizer of $i(E)$ in $\mathrm{End}^0(X)$. Clearly, $i(E)$ lies in the center of the finite-dimensional $\mathbf{Q}$-algebra $\mathrm{End}^0(X,i)$. It follows that $\mathrm{End}^0(X,i)$ carries a natural structure of finite-dimensional E-algebra. If Y is (possibly) another abelian variety over K_a and $j: E\hookrightarrow \mathrm{End}^0(Y)$ is an embedding that sends 1 to the identity automorphism of Y then we write

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

Clearly, $\mathrm{End}^0(X,i)=\mathrm{Hom}^0((X,i),(X,i))$. By abuse of language, we call elements of $\mathrm{Hom}^0((X,i),(Y,j))$ *E-equivariant* homomorphisms from X to Y.

Recall that if $\psi: X\to Y$ is an isogeny then there exist an isogeny $\phi: Y\to X$ and a positive integer N such that $\phi\psi = N1_X, \psi\phi = N1_Y$. One may easily check that if ψ is E-equivariant then ϕ is also E-equivariant.

If d is a positive integer then we write $i^{(d)}$ for the composition

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

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

One may easily check [23, Remark 4.1] that the E-algebra $\mathrm{End}^0(X,i)$ is semisimple. The following assertion is contained in [23, Theorem 4.2].

Theorem 3.1. (i) *We always have*

$$\dim_E(\mathrm{End}^0((X,i)) \le \frac{4\cdot\dim(X)^2}{[E:\mathbf{Q}]^2}.$$

(ii) *Suppose that*

$$\dim_E(\mathrm{End}^0((X,i)) = \frac{4\cdot\dim(X)^2}{[E:\mathbf{Q}]^2}.$$

Then X is an abelian variety of CM-type isogenous to a self-product of an (absolutely) simple abelian variety. Also $\mathrm{End}^0((X,i)$ is a central simple E-algebra, i.e., E coincides with the center of $\mathrm{End}^0((X,i)$.

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

Remark 3.2. Suppose that

$$\dim_E(\mathrm{End}^0((X,i)) = \frac{4\cdot\dim(X)^2}{[E:\mathbf{Q}]^2}.$$

By 3.1(ii), X is isogenous to a self-product of an absolutely simple abelian variety B. It is proven in [23, §4, Proof of Theorem 4.2] that B is an abelian variety of CM-type. Recall [12, Prop. 26 on p. 96] that in characteristic zero every absolutely simple abelian variety of CM type is defined over a number field; in positive characteristic such a variety is isogenous to an abelian variety defined over a finite field (a theorem of Grothendieck [5, Th. 1.1]). It follows easily that:

(1) If $\mathrm{char}(K)=0$ then X is defined over a number field;
(2) If $\mathrm{char}(K)>0$ then X is isogenous to an abelian variety defined over a finite field.

Let d be a positive integer that is not divisible by $\mathrm{char}(K)$. Suppose that X is defined over K. We write X_d for the kernel of multiplication by d in $X(K_a)$. It is known [4, Proposition on p. 64] that the commutative group X_d is a free $\mathbf{Z}/d\mathbf{Z}$-module of rank $2\dim(X)$. Clearly, X_d is a Galois submodule in $X(K_a)$. We write $\tilde{\rho}_{d,X}:\mathrm{Gal}(K)\to\mathrm{Aut}_{\mathbf{Z}/d\mathbf{Z}}(X_d)\cong\mathrm{GL}(2\dim(X),\mathbf{Z}/d\mathbf{Z})$ for the corresponding (continuous) homomorphism defining the Galois action on X_d. Let us put

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

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 $\ell \ne \mathrm{char}(K)$ then X_ℓ is a $2\dim(X)$-dimensional vector space over the prime field $\mathbf{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$ and the inclusion $\tilde{G}_{\ell,X} \subset \mathrm{Aut}_{\mathbf{F}_\ell}(X_\ell)$ defines a faithful linear representation of the group $\tilde{G}_{\ell,X}$ in the vector space X_ℓ.

Now let us assume that

$$i(\mathcal{O}) \subset \mathrm{End}_K(X).$$

Let λ 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 $\mathrm{char}(k(\lambda)) = \ell$ then $\lambda \supset \ell \cdot \mathcal{O}$ and therefore $X_\lambda \subset X_\ell$. Clearly, X_λ is a Galois submodule of X_ℓ. It is also clear that X_λ carries a natural structure of $\mathcal{O}/\lambda = k(\lambda)$-vector space. We write

$$\tilde{\rho}_{\lambda,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{k(\lambda)}(X_\lambda)$$

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

$$\tilde{G}_{\lambda,X} = \tilde{G}_{\lambda,i,X} := \tilde{\rho}_{\lambda,X}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{k(\lambda)}(X_\lambda).$$

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_λ.

In order to describe $\tilde{\rho}_{\lambda,X}$ explicitly, let us assume for the sake of simplicity that λ is the only maximal ideal of $\mathcal{O}$ dividing ℓ, i.e., $\ell \cdot \mathcal{O} = \lambda^b$ where the positive integer b satisfies $[E : \mathbf{Q}] = b \cdot [k(\lambda) : \mathbf{F}_\ell]$. Then $\mathcal{O} \otimes \mathbf{Z}_\ell = \mathcal{O}_\lambda$ where $\mathcal{O}_\lambda$ is the completion of $\mathcal{O}$ with respect to the λ-adic topology. It is well-known 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 λ^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 ℓ-adic Tate module of X defined as the projective limit of Galois modules X_{ℓ^m} [4, §18]. Recall that $T_\ell(X)$ is a free $\mathbf{Z}_\ell$-module of rank $2\dim(X)$

provided with the continuous action $\rho_{\ell,X}:\mathrm{Gal}(K)\to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X))$ and the natural embedding [4, §19, theorem 3]

$$\mathrm{End}_K(X)\otimes \mathbf{Z}_\ell \subset \mathrm{End}(X)\otimes \mathbf{Z}_\ell \hookrightarrow \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell(X)) \qquad (4).$$

Clearly, the image of $\mathrm{End}_K(X)\otimes \mathbf{Z}_\ell$ commutes with $\rho_{\ell,X}(\mathrm{Gal}(K))$. In particular, $T_\ell(X)$ carries the natural structure of $\mathcal{O}\otimes\mathbf{Z}_\ell=\mathcal{O}_\lambda$-module. The following assertion is a special case of Proposition 2.2.1 on p. 769 in [6].

Lemma 3.3. *The $\mathcal{O}_\lambda$-module $T_\ell(X)$ is free of rank r_X.*

There is also the natural isomorphism of Galois modules $X_\ell = T_\ell(X)/\ell T_\ell(X)$, which is also an isomorphism of $\mathrm{End}_K(X)\supset\mathcal{O}$-modules. This implies that the $\mathcal{O}[\mathrm{Gal}(K)]$-module X_λ coincides with

$$c^{-1}\ell T_\ell(X)/\ell T_\ell(X) = c^{b-1}T_\ell(X)/c^bT_\ell(X) = T_\ell(X)/cT_\ell(X) =$$

$$T_\ell(X)/\lambda T_\ell(X) = T_\ell(X)/(\lambda\mathcal{O}_\lambda)T_\ell(X).$$

Hence

$$X_\lambda = T_\ell(X)/(\lambda\mathcal{O}_\lambda)T_\ell(X) = T_\ell(X)\otimes_{\mathcal{O}_\lambda} k(\lambda),\ \dim_{k(\lambda)}X_\lambda = r_X = \frac{2\mathrm{dim}(X)}{[E:\mathbf{Q}]} \quad (5).$$

Let us consider the $2\mathrm{dim}(X)$-dimensional $\mathbf{Q}_\ell$-vector space

$$V_\ell(X) = T_\ell(X)\otimes_{\mathbf{Z}_\ell}\mathbf{Q}_\ell,$$

which carries a natural structure of r_X-dimensional E_λ-vector space. Extending the embedding (4) by $\mathbf{Q}_\ell$-linearity, we get the natural embedding

$$E\otimes_{\mathbf{Q}}\mathbf{Q}_\ell = \mathcal{O}\otimes\mathbf{Q}_\ell \overset{i}{\hookrightarrow} \mathrm{End}_K(X)\otimes\mathbf{Q}_\ell \subset \mathrm{End}^0(X)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbf{Q}_\ell}(V_\ell(X)).$$

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

Remark 3.4. (1) Clearly, the center $\mathfrak{C}_X$ of $\mathrm{End}^0(X)$ commutes with $i(E)$ and therefore lies in $\mathrm{End}^0(X,i)$. Since $\mathfrak{C}_X$ also commutes with $\mathrm{End}^0(X,i)$, it lies in the center of $\mathrm{End}^0(X,i)$;

(2) Notice that $E_\lambda = E\otimes_{\mathbf{Q}}\mathbf{Q}_\ell = \mathcal{O}\otimes\mathbf{Q}_\ell = \mathcal{O}_\lambda\otimes_{\mathbf{Z}_\ell}\mathbf{Q}_\ell$ is the field coinciding with the completion of E with respect to λ-adic topology. Clearly, $V_\ell(X)$ carries a natural structure of r_X-dimensional E_λ-vector space and $\dim_{E_\lambda}(\mathrm{End}_{E_\lambda}(V_\ell(X))) = r_X^2$.

(3) One may easily check that $\mathrm{End}^0(X,i)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell$ is a $E\otimes_{\mathbf{Q}}\mathbf{Q}_\ell=E_\lambda$-vector subspace (even subalgebra) in $\mathrm{End}_{E_\lambda}(V_\ell(X))$. Clearly,

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

(4) If $\mathrm{End}^0(X,i)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell=E_\lambda\mathrm{Id}$ then $\dim_E(\mathrm{End}^0(X,i))=1$ and, in light of the inclusion $E\cong i(E)\subset\mathrm{End}^0(X,i)$, we obtain that $\mathrm{End}^0(X,i)=i(E)$, i.e., $i(E)\cong E$ is a maximal commutative subalgebra in $\mathrm{End}^0(X)$ and $i(\mathcal{O})\cong\mathcal{O}$ is a maximal commutative subring in $\mathrm{End}(X)$. It follows that $\mathfrak{C}_X\subset i(E)$ and therefore is isomorphic to a subfield of E. In particular, $\mathfrak{C}_X$ is a field, i.e., $\mathrm{End}^0(X)$ is a simple $\mathbf{Q}$-algebra. This means that X is isogenous to a self-product of an absolutely simple abelian variety;

(5) Suppose that $\mathrm{End}^0(X,i)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell=\mathrm{End}_{E_\lambda}(V_\ell(X))$. This implies that

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

Applying Theorem 3.1, we conclude that X is an abelian variety of CM-type isogenous to a self-product of an (absolutely) simple abelian variety. Also $\mathrm{End}^0((X,i)$ is a central simple E-algebra, i.e., E coincides with the center of $\mathrm{End}^0((X,i)$. Moreover, if $\mathrm{char}(K_a)=0$ then $[E:\mathbf{Q}]$ is even and there exist a $\frac{[E:\mathbf{Q}]}{2}$-dimensional abelian variety Z, an isogeny $\psi:Z^r\to X$ and an embedding $k:E\hookrightarrow\mathrm{End}^0(Z)$ that send 1 to 1_Z and such that $\psi\in\mathrm{Hom}^0((Z^r,k^{(r)}),(X,i))$.

Using the inclusion $\mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X))\subset\mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(X))$, one may view $\rho_{\ell,X}$ as the ℓ-adic representation $\rho_{\ell,X}:\mathrm{Gal}(K)\to\mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X))\subset\mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(X))$.

Since X is defined over K, one may associate with every $u\in\mathrm{End}(X)$ and $\sigma\in\mathrm{Gal}(K)$ an endomorphism ${}^\sigma u\in\mathrm{End}(X)$ such that ${}^\sigma u(x)=\sigma u(\sigma^{-1}x)$ for all $x\in X(K_a)$. Clearly, ${}^\sigma u=u$ if $u\in\mathrm{End}_K(X)$. In particular, ${}^\sigma e=e$ if $e\in\mathcal{O}$ (here we identify $\mathcal{O}$ with $i(\mathcal{O})$). It follows easily that for each $\sigma\in\mathrm{Gal}(K)$ the map $u\mapsto{}^\sigma u$ extends by $\mathbf{Q}$-linearity to a certain automorphism of $\mathrm{End}^0(X)$. Clearly, ${}^\sigma e=e$ for each $e\in E$ and ${}^\sigma u\in\mathrm{End}^0(X,i)$ for each $u\in\mathrm{End}^0(X,i)$.

Remark 3.5. The definition of $T_\ell(X)$ as the projective limit of Galois modules X_{ℓ^m} implies that ${}^\sigma u(x)=\rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1}(x)$ for all $x\in T_\ell(X)$. It follows easily that ${}^\sigma u(x)=\rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1}(x)$ for all $x\in V_\ell(X),u\in\mathrm{End}^0(X),\sigma\in\mathrm{Gal}(K)$. This implies that for each $\sigma\in\mathrm{Gal}(K)$ we have $\rho_{\ell,X}(\sigma)\in\mathrm{Aut}_{E_\lambda}(V_\lambda(X))$ and therefore

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

[6, pp. 767–768] (see also [10]). It is also clear that $\rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1} \in \mathrm{End}^0(X)\otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ for all $u \in \mathrm{End}^0(X) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ and

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

We refer to [15, 16, 19, 21] for a discussion of the following definition.

Definition 3.6. Let V be a vector space over a field $\mathbf{F}$, let G be a group and $\rho : G \to \mathrm{Aut}_{\mathbf{F}}(V)$ a linear representation of G in V. We say that the G-module V is *very simple* if it enjoys the following property:

If $R \subset \mathrm{End}_{\mathbf{F}}(V)$ is an $\mathbf{F}$-subalgebra containing the identity operator Id such that $\rho(\sigma)R\rho(\sigma)^{-1} \subset R \quad \forall \sigma \in G$ then either $R = \mathbf{F} \cdot \mathrm{Id}$ or $R = \mathrm{End}_{\mathbf{F}}(V)$.

Remarks 3.7.
- (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 $H \twoheadrightarrow G$ 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 $\rho(G') \subset \mathrm{Aut}_k(V)$ consists of scalars (i.e., lies in $k \cdot \mathrm{Id}$) or the G'-module V is absolutely simple. See [19, 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, $\rho_F : G \to \mathrm{Aut}_F(V_F)$ 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 [19, Remark 5.2(v)].

Theorem 3.8. *Suppose that X is an abelian variety defined over K and $i(\mathcal{O}) \subset \mathrm{End}_K(X)$. Let ℓ be a prime different from* $\mathrm{char}(K)$. *Suppose that λ is the only maximal ideal dividing ℓ in $\mathcal{O}$. Suppose that the natural representation in the $k(\lambda)$-vector space X_λ is very simple. Then* $\mathrm{End}^0(X,i)$ *enjoys one of the following two properties:*

1. $\mathrm{End}^0(X,i) = i(E)$, *i.e., $i(E) \cong E$ is a maximal commutative subalgebra in* $\mathrm{End}^0(X)$ *and $i(\mathcal{O}) \cong \mathcal{O}$ is a maximal commutative subring in* $\mathrm{End}(X)$. *In particular, $i(E)$ contains the center of* $\mathrm{End}^0(X)$
2. *The following two conditions are fulfilled:*

(2a) $\mathrm{End}^0(X,i)$ *is a central simple* E*-algebra of dimension* r_X^2 *and* X *is an abelian variety of CM-type over* K_a.

(2b) *If* $\mathrm{char}(K)=0$ *then* $[E:\mathbf{Q}]$ *is even and there exist a* $\frac{[E:\mathbf{Q}]}{2}$*-dimensional abelian variety* Z*, an isogeny* $\psi: Z^r \to X$ *and an embedding* $k: E \hookrightarrow \mathrm{End}^0(Z)$ *that sends* 1 *to* 1_Z *and such that* $\psi \in \mathrm{Hom}^0((Z^r, k^{(r)}), (X,i))$*. In addition,* X *is defined over a number field.*
If $\mathrm{char}(K)>0$ *then* X *is isogenous to an abelian variety defined over a finite field.*

Proof. In light of 3.7(ii), the $\mathrm{Gal}(K)$-module X_λ is very simple. In light of 3.7(iv) and Remark 3.5, $\rho_{\ell,X}: \mathrm{Gal}(K) \to \mathrm{Aut}_{E_\lambda}(V_\ell(X))$ is also very simple. Let us put $R = \mathrm{End}^0(X,i) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$. It follows from Remark 3.5 that either $R = E_\lambda \mathrm{Id}$ or $R = \mathrm{End}_{E_\lambda}(V_\ell(X))$. Now the result follows readily from Remarks 3.4 and 3.2.

□

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 3.9. Suppose that Y is defined over K and $u \in \mathrm{End}_K(Y)$. Clearly, Z and the inclusion map $Z \subset Y$ are defined over $K_a^{\mathrm{Gal}(K)}$, i.e., Z and $Z \subset Y$ are defined over a purely inseparable extension of K. By a Theorem of Chow [2, Th. 5 on p. 26], Z is defined over K. Clearly, the graph of $Z \subset Y$ is an abelian subvariety of $Z \times Y$ defined over a purely inseparable extension of K. By the same Theorem of Chow, this graph is also defined over K and therefore $Z \subset Y$ is defined over K.

Theorem 3.10. *Let* Y *be an abelian variety of positive dimension over* K_a *and* δ *an automorphism of* Y*. Suppose that the induced* K_a*-linear operator* $\delta^*: \Omega^1(Y) \to \Omega^1(Y)$ *is diagonalizable. Let* S *be the set of eigenvalues of* δ^* *and* $\mathrm{mult}_Y: S \to \mathbf{Z}_+$ *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* δ*-invariant and we write* $\delta_Z: Z \to Z$ *for the corresponding automorphism of* Z *(i.e., for the restriction of* δ *to* z*). Suppose that*

$$\dim(Z) = \sum_{\lambda \in S, P(\lambda)\neq 0} \mathrm{mult}_Y(\lambda).$$

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* λ *of* δ_Z^* *equals* $mult_Y(\lambda)$.

Proof. Clearly, u commutes with δ. We write v for the (surjective) homomorphism $Y \twoheadrightarrow Z$ induced by u and j for the inclusion map $Z \subset Y$. Notice that $u : Y \to Y$ splits into a composition $Y \overset{v}{\twoheadrightarrow} Z \overset{j}{\hookrightarrow} Y$, i.e., $u = jv$. Clearly,

$$\delta_Z v = v\delta \in \mathrm{Hom}(Y,Z),\ j\delta_Z = \delta j \in \mathrm{Hom}(Z,Y),\ u = jv \in \mathrm{End}(Y),\ u\delta = \delta u \in \mathrm{End}(Y).$$

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

$$\sum_{\lambda \in S, P(\lambda) \neq 0} \mathrm{mult}_Y(\lambda) = \dim(Y)$$

and coincides with $\oplus_{\lambda \in S, P(\lambda)\neq 0} W_\lambda$ where W_λ is the eigenspace of δ attached to eigenvalue λ. Since $u^* = v^* j^*$, we have $u^*(\Omega^1(Y)) = v^* j^*(\Omega^1(Y)) \subset v^*(\Omega^1(Z))$. 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 γ the restriction of δ^* to $v^*(\Omega^1(Z))$ then $\gamma w = w\delta_Y^*$ and therefore $\gamma = w\delta_Y^* w^{-1}$. □

4. Cyclic covers and jacobians

Throughout this paper we fix a prime number p and an 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 $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Aut}(K_a/K)$. We also fix in K_a a primitive qth root of unity ζ.

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 $\mathrm{Gal}(L/K)$ is called the Galois group of f and denoted by $\mathrm{Gal}(f)$. Clearly, $\mathrm{Gal}(f)$ permutes elements of $\mathfrak{R}_f$ and the natural map of $\mathrm{Gal}(f)$ into the group $\mathrm{Perm}(\mathfrak{R}_f)$ of all permutations of $\mathfrak{R}_f$ is an embedding. We will identify $\mathrm{Gal}(f)$ with its image and consider it as a permutation group of $\mathfrak{R}_f$. Clearly, $\mathrm{Gal}(f)$ 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 [17, §3])

$$V_{f,p} := (\mathbf{F}_p^{\mathfrak{R}_f})^{00} = (\mathbf{F}_p^{\mathfrak{R}_f})^{0}$$

for the $(n-1)$-dimensional $\mathbf{F}_p$-vector space of functions $\{\phi : \mathfrak{R}_f \to \mathbf{F}_p,\ \sum_{\alpha\in\mathfrak{R}_f} \phi(\alpha) = 0\}$ provided with a natural action of the permutation group $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$. It is the *heart* over the field $\mathbf{F}_p$ of the group $\mathrm{Gal}(f)$ acting on the set $\mathfrak{R}_f$ [3, 17].

Remark 4.1. If p does not divide n and $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$ then the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. See [17, lemma 3.5].

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 $\pi : C \to \mathbf{P}^1$ of degree p. Let $B' \subset C(K_a)$ be the set of ramification points. Clearly, the restriction of π to B' is an *injective* map $B' \hookrightarrow \mathbf{P}^1(K_a)$, whose image is the disjoint union of ∞ 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, π is ramified at each point of B with ramification index q. We have $B' = B$ if n is divisible by q. 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 π at $\pi^{-1}(\infty)$ is also q. Using Hurwitz's formula, one may easily compute the genus $g = g(C) = g(C_{f,q})$ of C ([1, pp. 401–402], [13, proposition 1 on p. 3359], [7, 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)

$$\Delta_{n,q} := \{(j, i) \mid 0 \le j, \quad 0 \le i, \quad qj + ni \le nq\}$$

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 $(j, i) \in L_{n,q}$

$$1 \le j \le n-1; \quad 1 \le i \le q-1; \quad q(j-1) + (j+1) \le n(q-i).$$

Elementary calculations ([1, theorem 3 on p. 403]) show that

$$\omega_{j,i} := x^{j-1} dx/y^{q-i} = x^{j-1} y^i dx/y^q = x^{j-1} y^{i-1} dx/y^{q-1}$$

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, δ_q^q is the identity map and the set of fixed points of δ_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 [13, 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 δ_q. Notice also that if the Galois group of f over K is $\mathbf{S}_n$ (resp. $\mathbf{A}_n$) then the Galois group of h_1 over K_1 is $\mathbf{S}_{n-1}$ (resp. $\mathbf{A}_{n-1}$).

Remark 4.4. (i) It is well-known that $\dim_{K_a}(\Omega^1(C_{(f,q)})) = g(C_{f,q})$. By functoriality, δ_q induces on $\Omega^1(C_{(f,q)})$ a certain K_a-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 δ_q^* with eigenvalue ζ^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 ζ^{-i} of δ_q^* coincides with the number of interior integer points in $\Delta_{n,q}$ along the corresponding (to $q - i$) horizontal line. Elementary calculations show that this number is $\left[\frac{ni}{q}\right]$; in particular, ζ^{-i} *is an eigenvalue if and only if* $\left[\frac{ni}{q}\right] > 0$. Taking into account that $n \geq 4$ and $q = p^r$, we conclude that ζ^i is an eigenvalue of δ_q^* for each integer i with $p^r - p^{r-1} \leq i \leq p^r - 1 = q - 1$. It also follows easily that 1 is *not* an eigenvalue δ_q^*. This implies that

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

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

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) δ_q as an element of $\mathrm{Aut}(C) \subset \mathrm{Aut}(J(C)) \subset \mathrm{End}(J(C))$ such that $\delta_q \ne \mathrm{Id}$ but $\delta_q^q = \mathrm{Id}$ where Id is the identity endomorphism of $J(C)$. We write $\mathbf{Z}[\delta_q]$ for the subring of $\mathrm{End}(J(C))$ generated by δ_q.

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

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

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

Remark 4.6. Assume that p does not divide n. Clearly, the set S of eigenvalues λ of $\delta_q^* : \Omega^1(J(C_{f,q})) \to \Omega^1(J(C_{f,q}))$ with $\mathcal{P}_{q/p}(\lambda) \ne 0$ consists of *primitive* qth roots of unity ζ^{-i} $(1 \le i < q, (i,p) = 1)$ with $\left[\frac{ni}{q}\right] > 0$ and the multiplicity of ζ^{-i} equals $\left[\frac{ni}{q}\right]$, thanks to Remarks 4.5 and 4.4. Let us compute the sum

$$M = \sum_{1 \le i < q, (i,p)=1} \left[\frac{ni}{q}\right]$$

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

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

It follows easily that

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

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 δ_2 is the hyperelliptic involution $(x, y) \mapsto (x, -y)$. It is well-known that the differentials $x^i \frac{dx}{y}$ $(0 \le i \le g-1)$ constitute a basis of the g-dimensional $\Omega^1(J(C_{f,2}))$. It follows that δ_2^* is just multiplication by -1. Therefore

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

Clearly, 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 3.10.

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 $D = \mathrm{div}(h)$ where $h \in K_a(C)$ is a non-zero rational function of C. Since D is δ_q-invariant, the rational function $\delta_q^* h := h\delta_q$ coincides with $c\cdot h$ for some non-zero $c \in K_a$. It follows easily from the δ_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 $i \le q-1$. 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 $\mathrm{div}(y) = \sum_{P\in B}(P) - n(\infty)$. On the other hand, for each $\alpha \in \mathfrak{R}_f$, we have $P_\alpha = (\alpha, 0) \in B$ and the corresponding divisor $\mathrm{div}(x-\alpha) = q((\alpha,0)) - q(\infty) = q(P_\alpha) - q(\infty)$ is divisible by q. This implies that $a_{P_\alpha} = q\cdot b(\alpha) + i$. Also, since ∞ is neither zero no pole of h, we get the equality $0 = ni + \sum_{\alpha\in\mathfrak{R}_f} b(\alpha)q$. Since n and q are relatively prime, i must divide q. This implies that $i = 0$ and therefore the divisor $D = \mathrm{div}(u(x)) = \mathrm{div}(\prod_{\alpha\in\mathfrak{R}_f}(x-\alpha)^{b(\alpha)})$ 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 $D = \mathrm{div}(h)$. ◻

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

Proof. If $q = p$ is a prime this assertion is proven in [7, p. 149], [8, p. 458]. So, further we may assume that $q > p$. It follows from Remark 4.3 that we may assume that p does *not* divide n.

Now we follow arguments of [8, 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 $(\delta_q^{q-1}P) + \cdots + (\delta_q P) + (P) - q(\infty)$. This implies that $\mathcal{P}_q(\delta_q) = 0 \in \mathrm{End}(J(C_{f,q}))$.

Applying Remark 4.5(ii), we conclude that $\mathcal{P}_q(t)$ is the minimal polynomial of δ_q in $\mathrm{End}(J(C_{f,q}))$. $\square$

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 δ_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 Φ_q and $\mathcal{P}_{q/p}$ are relatively prime, the homomorphism $\mathcal{P}_{q/p}(\delta_q) : J^{(f,q)} \to J^{(f,q)}$ has finite kernel and therefore is an isogeny. In particular, it is surjective.

Lemma 4.11. *Suppose that p does not divide n. Then*

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

and there is an $K(\zeta)$-isogeny $J(C_{f,q}) \to J(C_{f,q/p}) \times J^{(f,q)}$. In addition, if $\zeta \in K$ 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 $\zeta \in K$. 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, π_1 induces a certain surjective homomorphism of jacobians $J(C_{f,q}) \twoheadrightarrow J(C_{f,q/p})$ which we continue to denote by π_1. Clearly, the equality $\pi_1\delta_q = \delta_{q/p}\pi_1$ remains true in $\mathrm{Hom}(J(C_{f,q}), J(C_{f,q/p}))$. By Lemma 4.8, $\mathcal{P}_{q/p}(\delta_{q/p}) = 0 \in \mathrm{End}(J(C_{f,q/p}))$. It follows from Lemma 4.10 that $\pi_1(J^{(f,q)}) = 0$ and therefore $\dim(J^{(f,q)})$ 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 4.7 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 want to prove that $(J^{(f,q)})^{\delta_q} = V_{f,p}$.

Recall that $J^{(f,q)}$ is δ_q-invariant and the restriction of δ_q to $J^{(f,q)}$ satisfies the qth cyclotomic polynomial. This allows us to define the homomorphism $\mathbf{Z}[\zeta_q] \to \mathrm{End}(J^{(f,q)})$ that sends 1 to the identity map and ζ_q to δ_q. Let us put $E = \mathbf{Q}(\zeta_q), \mathcal{O} = \mathbf{Z}[\zeta_q] \subset \mathbf{Q}(\zeta_q) = E$. It is well-known that $\mathcal{O}$ is the ring of integers in E, the ideal $\lambda = (1-\zeta_q)\mathbf{Z}[\zeta_q] = (1-\zeta_q)\mathcal{O}$ is maximal in $\mathcal{O}$ with $\mathcal{O}/\lambda = \mathbf{F}_p$ and $\mathcal{O} \otimes \mathbf{Z}_p = \mathbf{Z}_p[\zeta_q]$ is the ring of integers in the field $\mathbf{Q}_p(\zeta_q)$. Notice also that $\mathcal{O} \otimes \mathbf{Z}_p$ coincides with the completion $\mathcal{O}_\lambda$ of $\mathcal{O}$ with respect to the λ-adic topology and $\mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda = \mathcal{O}/\lambda = \mathbf{F}_p$.

It follows from Lemma 3.3 that

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

is a positive integer, the $\mathbf{Z}_p$-Tate module $T_p(J^{(f,q)})$ is a free $\mathcal{O}_\lambda$-module of rank d. Using the displayed formula (5) from §3, we conclude that

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

is a d-dimensional $\mathbf{F}_p$-vector space. Since $(J^{(f,q)})^{\delta_q}$ contains $(n-1)$-dimensional $\mathbf{F}_p$-vector space $V_{f,p}$, we have $d \ge n-1$. This implies that

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

and therefore

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

But we have already seen that

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

This implies that

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

It follows that $d = n-1$ and therefore $(J^{(f,q)})^{\delta_q} = V_{f,p}$. Dimension arguments imply that $J^{(f,q)}$ coincides with the identity component of $\ker(\pi_1)$ and therefore there is an isogeny between $J(C_{f,q})$ and $J(C_{f,q/p}) \times J^{(f,q)}$. □

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

Proof. Combine Corollary 4.11(ii) and Remark 4.9 with easy induction on 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 3.10 combined with Remark 4.6 that its spectrum consists of primitive qth roots of unity ζ^{-i} $(1 \le i < q)$ with $[ni/q] > 0$ and the multiplicity of ζ^{-i} equals $[ni/q]$.

Theorem 4.14. *Suppose that $n \ge 5$ is an integer. Let p be a prime, $r \ge 1$ 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 qth root of unity ζ. Let $f(x) \in K[x]$ be a separable polynomial of degree n and $\mathrm{Gal}(f)$ its Galois group. Suppose that the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. Then the image $\mathcal{O}$ of $\mathbf{Z}[\delta_q] \to \mathrm{End}(J^{(f,q)})$ is isomorphic to $\mathbf{Z}[\zeta_q]$ and enjoys one of the following two properties.*

- (i) *$\mathcal{O}$ is a maximal commutative subring in $\mathrm{End}(J^{(f,q)})$;*
- (ii) *$\mathrm{char}(K) > 0$ and the centralizer of $\mathcal{O} \otimes \mathbf{Q} \cong \mathbf{Q}(\zeta_q)$ in $\mathrm{End}^0(J^{(f,q)})$ is a central simple $(n-1)^2$-dimensional $\mathbf{Q}(\zeta_q)$-algebra. In addition, $J^{(f,q)}$ is an abelian variety of CM-type isogenous to a self-product of an absolutely simple abelian variety. Also $J^{(f,q)}$ is isogenous to an abelian variety defined over a finite field.*

Proof. Clearly, $\mathcal{O}$ is isomorphic to $\mathbf{Z}[\zeta_q]$. Let us put $\lambda = (1-\zeta_q)\mathbf{Z}[\zeta_q]$. By Lemma 4.11(iii), the Galois module $(J^{(f,q)})^{\delta_q} = J_\lambda^{(f,q)}$ is isomorphic to $V_{f,p}$. Applying Theorem 3.8, we conclude that either (ii) holds true or one of the following conditions hold:

- (a) $\mathcal{O}$ is a maximal commutative subring in $\mathrm{End}(J^{(f,q)})$;
- (b) $\mathrm{char}(K) = 0$ and there exist a $\varphi(q)/2$-dimensional abelian variety Z over K_a, an embedding $\mathbf{Q}(\zeta_q) \hookrightarrow \mathrm{End}^0(Z)$ that sends 1 to 1_Z and a $\mathbf{Q}(\zeta_q)$-equivariant isogeny $\psi: Z^{n-1} \to J^{(f,q)}$.

Clearly, if (a) is fulfilled then we are done. Also if $q = 2$ then $\varphi(q)/2 = 1/2$ is not an integer and therefore (b) is not fulfilled, i.e. (a) is fulfilled.

So further we assume that $q > 2$ and (b) holds true. In particular, $\mathrm{char}(K) = 0$. We need to arrive to a contradiction.

Since $\mathrm{char}(K) = 0$, the isogeny ψ induces an isomorphism $\psi^*: \Omega^1((J^{(f,q)})) \cong \Omega^1(Z^{n-1})$ that commutes with the actions of $\mathbf{Q}(\zeta_q)$. Since

$$\dim(\Omega^1(Z)) = \dim(Z) = \frac{\varphi(q)}{2},$$

the linear operator in $\Omega^1(Z)$ induced by $\zeta_q \in \mathbf{Q}(\zeta_q)$ has, at most, $\varphi(q)/2$ distinct eigenvalues. It follows that the linear operator in $\Omega^1(Z^{n-1}) = \Omega^1(Z)^{n-1}$ induced by ζ_q also has, at most, $\varphi(q)/2$ distinct eigenvalues. This implies that the linear operator δ_q^* in $\Omega^1((J^{(f,q)}))$ also has, at most, $\varphi(q)/2$ distinct eigenvalues. Recall that the eigenvalues of δ_q^* are primitive qth roots of unity ζ^{-i} with

$$1 \le i < q, (i,p) = 1, \left[\frac{ni}{q}\right] > 0.$$

Clearly, the inequality $[ni/q] > 0$ means that $i > q/n$, since $(n,q) = (n,p^r) = 1$. So, in order to get a desired contradiction, it suffices to check that the cardinality of the set

$$B := \left\{ i \in \mathbf{Z} \mid \frac{q}{n} < i < q = p^r, (i,p) = 1 \right\}$$

is strictly greater than $(p-1)p^{r-1}/2$. Since $p \ge 2, n \ge 5$ and q/n is not an integer, we have

$$\frac{p}{n} \le \frac{p}{5} < \frac{p-1}{2}$$

and

$$\#(B) > \varphi(q) - \frac{q}{n} = (p-1)p^{r-1} - \frac{p^{r-1}p}{n} \ge \left(p - 1 - \frac{p}{5}\right) p^{r-1} > \frac{p-1}{2} p^{r-1}.$$

□

Corollary 4.15. *Suppose that $n \ge 5$ is an integer. Let p be a prime, $r \ge 1$ an integer and $q = p^r$. Assume in addition that either p does not divide n or $q \mid n$ and $(n,q) \ne (5,5)$. 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 $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$. Then the image $\mathcal{O}$ of $\mathbf{Z}[\delta_q] \to \mathrm{End}(J^{(f,q)})$ is isomorphic to $\mathbf{Z}[\zeta_q]$ and enjoys one of the following two properties.*

(i) *$\mathcal{O}$ is a maximal commutative subring in $\mathrm{End}(J^{(f,q)})$;*
(ii) *$\mathrm{char}(K) > 0$ and the centralizer of $\mathcal{O} \otimes \mathbf{Q} \cong \mathbf{Q}(\zeta_q)$ in $\mathrm{End}^0(J^{(f,q)})$ is a central simple $(n-1)^2$-dimensional $\mathbf{Q}(\zeta_q)$-algebra. In addition, $J^{(f,q)}$ is an abelian variety of CM-type isogenous to a self-product of an absolutely simple abelian variety.*

Proof. If p divides n then $n > 5$ and therefore $n - 1 \ge 5$. By Remark 4.3, we may assume that p does not divide n. If we replace K by $K(\zeta)$ then still $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$. By Remark 4.1 if $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$ then the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. One has only to apply Theorem 4.14. □

Theorem 4.16. *Suppose $n \ge 4$ and p does not divide n. Assume also that* $\mathrm{char}(K) = 0$ *and* $\mathbf{Q}[\delta_q]$ *is a maximal commutative subalgebra in* $\mathrm{End}^0(J^{(f,q)})$. *Then* $\mathrm{End}^0(J^{(f,q)}) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}(\zeta_q)$ *and therefore* $\mathrm{End}(J^{(f,q)}) = \mathbf{Z}[\delta_q] \cong \mathbf{Z}[\zeta_q]$. *In particular, $J^{(f,q)}$ is an absolutely simple abelian variety.*

Proof. Let $\mathfrak{C} = \mathfrak{C}_{J^{(f,p)}}$ be the center of $\mathrm{End}^0(J^{(f,p)})$. Since $\mathbf{Q}[\delta_q]$ is a maximal commutative subalgebra, $\mathfrak{C} \subset \mathbf{Q}[\delta_q]$.

Replacing, if necessary, K by its subfield (finitely) generated over $\mathbf{Q}$ by all the coefficients of f, we may assume that K (and therefore K_a) is isomorphic to a subfield of $\mathbf{C}$. So, $K \subset K_a \subset \mathbf{C}$. We may also assume that $\zeta = \zeta_q$ and consider $J^{(f,q)}$ as complex abelian variety. Let $\Sigma = \Sigma_E$ be the set of all field embeddings $\sigma : E = \mathbf{Q}[\delta_q] \hookrightarrow \mathbf{C}$. We are going to apply Corollary 2.2 to $Z = J^{(f,q)}$ and $E = \mathbf{Q}[\delta_q]$. In order to do that we need to get some information about the multiplicities $n_\sigma = n_\sigma(Z, E) = n_\sigma(J^{(f,q)}, \mathbf{Q}[\delta_q])$. The displayed formula (1) in §2 allows us to do it, using the action of $\mathbf{Q}[\delta_q]$ on $\Omega^1(J^{(f,q)})$. Namely, since δ_q generates the field E (over $\mathbf{Q}$), each $\Omega^1(J^{(f,q)})_\sigma$ is the eigenspace corresponding to the eigenvalue $\sigma(\delta_q)$ of δ_q and n_σ is the multiplicity of the eigenvalue $\sigma(\delta_q)$.

Let $i < q$ be a positive integer that is not divisible by p and $\sigma_i : \mathbf{Q}[\delta_q] \hookrightarrow \mathbf{C}$ be the embedding which sends δ_q to ζ^{-i}. Clearly, for each σ there exists precisely one i such that $\sigma = \sigma_i$. Clearly, $\Omega^1(J^{(f,q)})_{\sigma_i}$ is the eigenspace of $\Omega^1(J^{(f,q)})$ attached to the eigenvalue ζ^{-i} of δ_q. Therefore n_{σ_i} coincides with the multiplicity of the eigenvalue ζ^{-i}. It follows from Remark 4.13 that

$$n_{\sigma_i} = \left[\frac{ni}{q}\right].$$

Now the assertion of the Theorem follows from Corollary 2.2 applied to $E = \mathbf{Q}[\delta_q] \cong \mathbf{Q}(\zeta_q)$. □

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 $n \ge 5$ and* $\mathrm{Gal}(f) = \mathbf{S}_n$ *or* $\mathbf{A}_n$. *Assume also that either p does not divide n or q divides n. Then* $\mathrm{End}^0(J^{(f,q)}) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}(\zeta_q)$ *and therefore* $\mathrm{End}(J^{(f,q)}) = \mathbf{Z}[\delta_q] \cong \mathbf{Z}[\zeta_q]$. *In particular, $J^{(f,q)}$ is an absolutely simple abelian variety.*

Proof. If $(n, q) \ne (5, 5)$ then the assertion follows from Corollary 4.15 combined with Corollary 4.16. The case $(n, q) = (5, 5)$ is contained in [20, theorem 4.2]. □

Corollary 4.18. *Let p be a prime and K a field of characteristic zero. Suppose that $f(x) \in K[x]$ is an irreducible polynomial of degree $n \ge 5$ and* $\mathrm{Gal}(f) = \mathbf{S}_n$ *or*

$\mathbf{A}_n$. *Let r and s be distinct positive integers. Assume also that either p does not divide n or both p^r and p^s divide n. Then* $\mathrm{Hom}(J^{(f,p^r)}, J^{(f,p^s)}) = 0$.

Proof. It follows from Theorem 4.17 that $J^{(f,p^r)}$ and $J^{(f,p^s)}$ are absolutely simple abelian varieties, whose endomorphism algebras $\mathbf{Q}(\zeta_{p^r})$ and $\mathbf{Q}(\zeta_{p^s})$ are not isomorphic. Therefore these abelian varieties are not isogenous. Since they are absolutely simple, every homomorphism between them is zero. □

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

Theorem 4.19. *Let p be a prime, r a positive integer, $q = p^r$. Suppose that K is a field of characteristic zero containing a primitive qth root of unity. Let $f(x) \in K[x]$ be a polynomial of degree $n \geq 5$. Assume also that p does not divide n and the* $\mathrm{Gal}(f)$*-module $V_{f,p}$ is very simple. Then* $\mathrm{End}^0(J^{(f,q)}) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}(\zeta_q)$ *and therefore* $\mathrm{End}(J^{(f,q)}) = \mathbf{Z}[\delta_q] \cong \mathbf{Z}[\zeta_q]$. *In particular, $J^{(f,q)}$ is an absolutely simple abelian variety.*

Corollary 4.20. *Let p be a prime, and K a field of characteristic zero. Let $f(x) \in K[x]$ be a polynomial of degree $n \geq 5$. Assume also that p does not divide n and the* $\mathrm{Gal}(f)$*-module $V_{f,p}$ is very simple. If r and s are distinct positive integers such that K contains primitive p^rth and p^sth roots of unity then* $\mathrm{Hom}(J^{(f,p^r)}, J^{(f,p^s)}) = 0$.

Proof. It follows from Theorem 4.19 that $J^{(f,p^r)}$ and $J^{(f,p^s)}$ are absolutely simple abelian varieties, whose endomorphism algebras $\mathbf{Q}(\zeta_{p^r})$ and $\mathbf{Q}(\zeta_{p^s})$ are not isomorphic. Therefore these abelian varieties are not isogenous. Since they are absolutely simple, every homomorphism between them is zero. □

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 qth 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 $\mathrm{Gal}(f) = \mathrm{Gal}(K(\mathfrak{R}_f)/K) \subset \mathrm{Perm}(\mathfrak{R}_f)$. Let r be a positive integer. Recall (Corollary 4.12) that if p does not divide n then there is a $K(\zeta_{p^r})$-isogeny $J(C_{f,p^r}) \to \prod_{i=1}^{r} J^{(f,p^i)}$. Applying Theorem 4.19 and Corollary 4.20 to all $q = p^i$, we obtain the following assertion.

Theorem 5.1. *Let p be a prime, r a positive integer, $q = p^r$. Suppose that K is a field of characteristic zero containing a primitive p^rth root of unity. Let*

$f(x) \in K[x]$ be an polynomial of degree $n \geq 5$. Assume also that p does not divide n and the $\mathrm{Gal}(f)$*-module $V_{f,p}$ is very simple. Then* $\mathrm{End}^0(J(C_{f,q})) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

The next statement obviously generalizes Theorem 1.1.

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* $\mathrm{Gal}(f) = \mathbf{S}_n$ *or* $\mathbf{A}_n$. *Assume also that either p does not divide n or $q \mid n$. Then* $\mathrm{End}^0(J(C_{f,q})) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

Proof. The existence of the isogeny $J(C_{f,q}) \to \prod_{i=1}^r J^{(f,p^i)}$ combined with Theorem 4.17 and Corollary 4.18 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 $L = \mathbf{C}(z_1, \cdots, z_n)$ is the field of rational functions in n independent variables $z_1, \cdots, z_n$ with constant field $\mathbf{C}$ and $K = L^{\mathbf{S}_n}$ 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 $\mathbf{S}_n$. Let 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 $\prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

Example 5.4. Let $h(x) \in \mathbf{C}[x]$ 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.) If $K = \mathbf{C}(z)$ then a theorem of Hilbert ([11, theorem 4.4.5, p. 41]) asserts that the Galois group of $h(x) - z$ over K is $\mathbf{S}_n$. 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 $\prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

References

[1] J. K. Koo, *On holomorphic differentials of some algebraic function field of one variable over* C. Bull. Austral. Math. Soc. **43** (1991), 399–405.

[2] S. Lang, Abelian varieties, 2nd edition, Springer Verlag, 1983.

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

[4] D. Mumford, Abelian varieties, 2nd edition, Oxford University Press, 1974.

[5] F. Oort, *The isogeny class of a CM-abelian variety is defined over a finite extension of the prime field*. J. Pure Applied Algebra **3** (1973), 399–408.

[6] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*. Amer. J. Math. 98 (1976), 751–804.

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

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

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

[10] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves, 3rd edition. AK Peters, Wellesley, 1998.

[11] J.-P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, 1992.

[12] G. Shimura, Abelian varieties with complex nmultiplication and modular functions, Princeton University Press, Princeton, 1997.

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

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

[15] 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.

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

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

[18] 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.

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

[20] Yu. G. Zarhin, *The endomorphism rings of jacobians of cyclic covers of the projective line*. Math. Proc. Cambridge Philos. Soc. **136** (2004), 257–267.

[21] Yu. G. Zarhin, *Very simple representations: variations on a theme of Clifford*. In: Progress in Galois Theory Conference (H. Völklein, T. Shaska eds.), Kluwer Academic Publishers, 2004, pp. 151–168.

[22] Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians*. Bull. Soc. Math. France, to appear.

[23] Yu. G. Zarhin, *Homomorphisms of abelian varieties*. e-print: http://arXiv.org/abs/math/0406273; to appear in: Proceedings of the "Arithmetic, Geometry and Coding Theory - 9" conference.

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

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