JACOBIANS WITH AUTOMORPHISMS OF PRIME ORDER

YURI G. ZARHIN

Abstract. In this paper we study principally polarized abelian varieties that admit an automorphism of prime order \( p > 2 \). It turns out that certain natural conditions on the multiplicities of its action on the differentials of the first kind do guarantee that those polarized varieties are not jacobians of curves.

1. Principally polarized abelian varieties with automorphisms

We write \( \mathbb{Z}_+ \) for the set of nonnegative integers, \( \mathbb{Q} \) for the field of rational numbers and \( \mathbb{C} \) for the field of complex numbers. We have

\[
\mathbb{Z}_+ \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}
\]

where \( \mathbb{Z} \) is the ring of integers and \( \mathbb{R} \) is the field of real numbers. If \( B \) is a finite (may be, empty) set then we write \( \#(B) \) for its cardinality. Let \( p \) be an odd prime and \( \zeta_p \in \mathbb{C} \) a primitive (complex) \( p \)th root of unity. It generates the multiplicative order \( p \) cyclic group \( \mu_p \) of \( p \)th roots of unity. We write \( \mathbb{Z}[\zeta_p] \) and \( \mathbb{Q}(\zeta_p) \) for the \( p \)th cyclotomic ring and the \( p \)th cyclotomic field respectively. We have

\[
\zeta_p \in \mu_p \subset \mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p) \subset \mathbb{C}.
\]

Let \( g \geq 1 \) be an integer and \((X, \lambda)\) a principally polarized \( g \)-dimensional abelian variety over the field \( \mathbb{C} \) of complex numbers, \( \delta \) an automorphism of \((X, \lambda)\) that satisfies the cyclotomic equation \( \sum_{j=0}^{p-1} \delta^j = 0 \) in \( \text{End}(X) \). In other words, \( \delta \) is a periodic automorphism of order \( p \), whose set of fixed points is finite. This gives rise to the embeddings

\[
\mathbb{Z}[\zeta_p] \hookrightarrow \text{End}(X), \ 1 \mapsto 1_X, \ \zeta_p \mapsto \delta,
\]

\[
\mathbb{Q}(\zeta_p) \hookrightarrow \text{End}^0(X), \ 1 \mapsto 1_X, \ \zeta_p \mapsto \delta.
\]

Since the degree \( [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 \), it follows from [10] Ch. 2, Prop. 2 (see also [9] Part II, p. 767) that

\[
(p - 1) \mid 2g.
\]

By functoriality, \( \mathbb{Q}(\zeta_p) \) acts on the \( g \)-dimensional complex vector space \( \Omega^1(X) \) of differentials of the first kind on \( X \). This provides \( \Omega^1(X) \) with a structure of \( \mathbb{Q}(\zeta_p) \otimes \mathbb{Q} \mathbb{C}\)-module. Clearly,

\[
\mathbb{Q}(\zeta_p) \otimes \mathbb{Q} \mathbb{C} = \bigoplus_{j=1}^{p-1} \mathbb{C}
\]

where the \( j \)th summands corresponds to the field embedding \( \mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C} \) that sends \( \zeta_p \) to \( \zeta_p^j \). So, \( \mathbb{Q}(\zeta_p) \) acts on \( \Omega^1(X) \) with multiplicities \( a_j \ (j = 1, \ldots, p - 1) \). Clearly,
all $a_j$ are non-negative integers and

$$\sum_{j=1}^{p-1} a_j = g. \tag{2}$$

In addition,

$$a_j + a_{p-j} = \frac{2g}{p-1} \text{ for all } j = 1, \ldots, p-1; \tag{3}$$

this is a special case of a general well known result about endomorphism fields of complex abelian varieties: see, e.g., [6, p. 84].

We may view $\{a_j\}$ as a nonnegative integer-valued function $a = a_X$ on the finite cyclic group $G = (\mathbb{Z}/p\mathbb{Z})^*$ of order $(p-1)$ where

$$a(j \mod p) = a_j \ (1 \leq j \leq p-1), \quad \sum_{h \in G} a(h) = g. \tag{4}$$

The group $G$ contains two distinguished elements, namely, the identity element $1 \mod p$ and the only element $(-1) \mod p = (p-1) \mod p$ of order 2. If $h$ is an element of $G$ then we write $-h$ for the product $(-1) \mod p \cdot h$ in $G$. If $h = j \mod p$ then $-h = (p-j) \mod p$. In light of (3),

$$a_X(h) + a_X(-h) = \frac{2g}{p-1} \quad \text{for all } h \in G. \tag{5}$$

**Definition 1.1.** Let $f : G \to \mathbb{Z}_+$ be a nonnegative integer-valued function. We say that $f$ is admissible if

$$a(h) + a(-h) = \frac{2g}{p-1} \quad \forall h \in G.$$

**Remark 1.2.**

(i) In light of (i), our $a = a_X$ is admissible.

(ii) The number of admissible functions (for given $g$ and $p$) is obviously

$$\left(\frac{2g}{p-1} + 1\right)^{(p-1)/2}.$$

**Example 1.3.** Let $p = 3$ and $E$ an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathbb{Z}[\zeta_3]$. We may take as $E$ the smooth projective model of $y^2 = x^3 - 1$ where $\gamma_3$ acts on $E$ by

$$\delta_E : (x, y) \mapsto (x, \gamma_3 y).$$

Clearly, $\delta_E$ satisfies the 3rd cyclotomic equation and respects the only principal polarization on $E$.

Let $g$ be a positive integer, and $f(1)$ and $f(-1)$ are nonnegative integers, whose sum is $g$. Let us put

$$Y_1 = E^{f(1)}, \ Y_2 = E^{f(2)}, \ Y = Y_1 \times Y_2.$$ 

Let $\lambda_Y$ be the principal polarization on $Y$ that is the product of $g$ pull-backs of the polarization on $E$. Let us consider the automorphism $\delta_{3}$ of $Y$ that acts (diagonally) as $\delta_E$ on $Y_1 = E^{f(1)}$ and as $\delta_{E}^{-1}$ on $Y_2 = E^{f(2)}$. Clearly, $\delta_{3}$ satisfies the 3rd cyclotomic equation and respects $\lambda_Y$. It is also clear that

$$a_Y(1) = f(1), a_Y(1) = f(2).$$
We will also need the function
\[
j: G = (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}, \ (j \ mod \ p) \mapsto j \ (1 \leq j \leq p-1).
\]
Clearly,
\[
j(h_1h_2) \equiv j(h_1)j(h_2) \ mod \ p \ \forall h_1, h_2 \in G.
\]
Recall that if \(f_1(h)\) and \(f_2(h)\) are complex-valued functions on \(G\) then its convolution is the function \(f_1 * f_2(h)\) on \(G\) defined by
\[
f_1 * f_2(h) = \frac{1}{p-1} \sum_{v \in G} f_1(u)f_2(u^{-1}h).
\]

**Theorem 1.4.** Suppose that \((X, \lambda)\) is the Jacobian of a smooth projective irreducible genus \(g\) curve \(C\) with canonical principal polarization. Then there exists a nonnegative integer-valued function \(b : G = (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z} \subset C\) such that
\[
\sum_{h \in G} b(h) = \frac{2g}{p-1} + 2,
\]
\[
a(v) = \frac{(p-1)}{p} \cdot b \cdot j(-v) - 1 \ \forall \ v \in G.
\]

**Proof.** Suppose that \((X, \lambda) \cong (J(C), \Theta)\) where \(C\) is an irreducible smooth projective genus \(g\) curve, \(J(C)\) its Jacobian with canonical principal polarization \(\Theta\). It follows from the Torelli theorem in Weil’s form \([11, 12]\) that there exists an automorphism \(\phi : C \to C\), which induces (by functoriality) either \(\delta\) or \(-\delta\) on \(J(C) = X\). Replacing \(\phi\) by \(\phi^{p+1}\) and taking into account that \((p+1)\) is even and \(\delta^p\) is the identity automorphism of \(X = J(C)\), we may and will assume that \(\phi\) induces \(\delta\). Clearly, \(\phi^p\) is the identity automorphism of \(C\), because it induces the identity map on \(J(C)\) and \(g > 1\). The action of \(\phi\) on \(C\) gives rise to the group embedding
\[
\mu_p \hookrightarrow \text{Aut}(C), \ \zeta_p \mapsto \phi.
\]

Let \(P \in C\) be a fixed point of \(\phi\). Then \(\phi\) induces the automorphism of the corresponding (one-dimensional) tangent space \(T_P(C)\), which is multiplication by a complex number \(\epsilon_P\). Clearly, \(\epsilon_P\) is a \(p\)th root of unity.

The following result is well known (see, e.g., \([14]\)).

**Lemma 1.5.** Every fixed point \(P\) of \(\phi\) is nondegenerate, i.e., \(\epsilon_P \neq 1\).

**Corollary 1.6.** The quotient \(D := C/\mu_p\) is a smooth projective irreducible curve. The map \(C \to D\) has degree \(p\), its ramification points are exactly the images of fixed points of \(\phi\) and all the ramification indices are \(p\).

**Lemma 1.7.** \(D\) is biregularly isomorphic to the projective line.

**Proof of Lemma 1.7.** The map \(C \to D\) induces, by Albanese functoriality, the surjective homomorphism of the corresponding Jacobians \(J(C) \to J(D)\) that kills the divisors classes of the form \((Q) - (\phi(Q))\) for all \(Q \in C(C)\). This implies that it kills \((1 - \delta)J(C)\). On the other hand, \(1 - \delta : J(C) \to J(C)\) is, obviously, an isogeny. This implies that the image of \(J(C)\) in \(J(D)\) is zero and the surjectiveness implies that \(J(D) = 0\). This means that the genus of \(D\) is 0. \(\square\)
Corollary 1.8. The number $F(\phi)$ of fixed points of $\phi$ is $\frac{2g}{p-1} + 2$.

Proof of Corollary 1.8. Applying the Riemann-Hurwitz’s formula to $C \to D$, we get

$$2g - 2 = p \cdot (-2) + (p - 1) \cdot F(\phi).$$

Lemma 1.9. Let $\phi^* : \Omega^1(C) \to \Omega^1(C)$ be the automorphism of the $g$-dimensional complex vector space $\Omega^1(C)$ induced by $\phi$ and $\tau$ the trace of $\phi^*$. Then

$$\tau = \sum_{j=1}^{p-1} a_j \zeta_j^p = \sum_{h \in G} a(h) \zeta_h^p.$$ 

Proof of Lemma 1.9. Pick a $\phi$-invariant point $P_0$ and consider the regular map $\alpha : C \to J(C), Q \mapsto \text{cl}((Q) - (P_0))$.

It is well-known that $\alpha$ induces an isomorphism of complex vector spaces $\alpha^* : \Omega^1(J(C)) \cong \Omega^1(C)$.

Clearly, $\phi^* = \alpha^* \delta^* \alpha^{-1}$

where $\delta^* : \Omega^1(J(C)) = \Omega^1(J(C))$ is the $\mathbb{C}$-linear automorphism induced by $\delta$. This implies that the traces of $\phi^*$ and $\delta^*$ do coincide. Now the very definition of $a_j$’s implies that the trace of $\phi^*$ equals $\sum_{j=1}^{p-1} a_j \zeta_j^p$. \qed

Lemma 1.10. Let $\zeta \in \mathbb{C}$ be a primitive $p$th root of unity. Then

$$(11) \quad \frac{1}{1 - \zeta} = - \frac{\sum_{j=1}^{p-1} j \zeta_j^i}{p} = - \sum_{h \in G} \zeta_h^i.$$ 

Proof. We have

$$(1 - \zeta) \left( \sum_{j=1}^{p-1} j \zeta_j^i \right) = \sum_{j=1}^{p-1} \left( j \zeta_j^i - j \zeta_j^{i+1} \right) = \left( \sum_{j=1}^{p-1} \zeta_j^i \right) - (p-1) \zeta^p = (-1) - (p-1) = -p. \quad \Box$$

End of proof of Theorem 1.4. Let $B$ be the set of fixed points of $\phi$. We know that $\#(B) = \frac{2g}{p-1} + 2$. By the holomorphic Lefschetz fixed point formula [1, Th. 2], [2, Ch. 3, Sect. 4] (see also [5, Sect. 12.2 and 12.5]) applied to $\phi$,

$$(12) \quad 1 - \tau = \sum_{P \in B} \frac{1}{1 - \epsilon_P}$$ 

where $\bar{\tau}$ is the complex-conjugate of $\tau$. Recall that every $\epsilon_P$ is a (primitive) $p$th root of unity. Now Theorem 1.4 follows readily from the following assertion.

Proposition 1.11. Let us define for each $h \in G$ the nonnegative integer $b(h)$ as the number of fixed points $P \in B \subset C(C)$ such that $\epsilon_P = \zeta_h^p$. Then

$$(13) \quad \sum_{h \in G} b(h) = F(\phi) = \frac{2g}{p-1} + 2.$$
JACOBIANS WITH AUTOMORPHISMS OF PRIME ORDER

and

\[ a(v) = \frac{(p-1)}{p} \cdot b \ast j(-v) - 1 \forall v \in G. \]

\[ \Box \]

**Proof of Proposition 1.11.** The equality (13) is obvious. Let us prove (14). Combining (12) with Lemma 1.10 (applied to \( \zeta = \zeta^h_p \)) and Lemma 1.9, we get

\[
1 - \sum_{h \in G} a(h)\zeta^{-h}_p = \sum_{u \in G} b(u) \frac{1}{1 - \zeta^u_p} = -\frac{1}{p} \left( \sum_{u \in G} b(u) \left( \sum_{h \in G} j(h)\zeta^h_p \right) \right) = \]

\[
-\frac{1}{p} \sum_{v \in G} \left( \sum_{u \in G} b(u)j(u^{-1}v) \right) \zeta^v_p = -\frac{1}{p} \sum_{v \in G} b \ast j(v)\zeta^v_p
\]

(here we use a substitution \( v = hu \)). Taking into account that

\[
0 = 1 + \sum_{j=1}^{p-1} \zeta^j_p = 1 + \sum_{v \in G} \zeta^v_p,
\]

we obtain

\[
- \left( \sum_{v \in G} \zeta^v_p \right) - \sum_{h \in G} a(h)\zeta^{-h}_p = -\frac{(p-1)}{p} \sum_{v \in G} b \ast j(v)\zeta^v_p.
\]

Taking into account that the \((p-1)\)-element set

\[ \{ \zeta^j_p \mid 1 \leq j \leq p-1 \} = \{ \zeta^v_p \mid v \in G \} \]

is a basis of the \( \mathbb{Q} \)-vector space \( \mathbb{Q}(\zeta_p) \), we get

\[ 1 + a(-v) = (p-1)b \ast j(v)/p, \]

i.e.,

\[ a(v) = \frac{(p-1)}{p} \cdot b \ast j(-v) - 1 \forall v \in G. \]

\[ \Box \]

**Remark 1.12.** Let us consider the function

\[ j_0 = j - \frac{p}{2} : G = (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Q}, \ (j \mod p) \mapsto j - \frac{p}{2} \quad \text{where} \quad j = 1, \ldots, p-1. \]

Then

\[ j_0(-u) = -j_0(u) \forall u \in G. \]

We have

\[ b \ast j(v) = b \ast j_0(v) + \frac{p}{2(p-1)} \sum_{h \in G} b(h) = b \ast j_0(v) + \frac{p}{2(p-1)} \left( \frac{2g}{p-1} + 2 \right). \]

This implies that

\[ \frac{(p-1)}{p} \cdot b \ast j(v) = \frac{(p-1)}{p} \cdot b \ast j_0(v) + \frac{g}{p-1} + 1 \]

and therefore

\[ a(v) = \frac{(p-1)}{p} \cdot b \ast j_0(-v) + \frac{g}{p-1} \forall v \in G. \]

On the other hand, It follows from (16) that the convolution \( b \ast j_0 \) also satisfies

\[ b \ast j_0(-v) = b \ast j_0(v) \forall v \in G. \]
This implies that
\[ a(v) + a(-v) = \frac{(p - 1)}{p} \cdot b \ast j_0(-v) + g \cdot \frac{(p - 1)}{p} \cdot b \ast j_0(v) = \frac{2g}{p - 1} \forall v \in G. \]

This implies that
\[ a(v) + a(-v) = \frac{2g}{p - 1}. \]

(Actually, we already know it, see (3).) It follows from (18) that
\[ a(v) = \frac{2g}{p - 1} - \frac{(p - 1)}{p} \cdot b \ast j(v) + 1 \forall v \in G. \]

**Corollary 1.13.** We keep the notation and assumptions of Theorem 1.4. Let 
\[ b' : G \to \mathbb{C} \]
be a complex-valued function on \( G \) such that
\[ a(v) = \frac{(p - 1)}{p} \cdot b' \ast (-v) - 1. \]

Then the odd parts of functions \( b \) and \( b' \) do coincide, i.e.
\[ b'(v) - b'(-v) = b(v) - b(-v). \]
In particular, if \( p = 3 \) then
\[ b'(v) = b(v) \forall v \in G. \]

**Proof.** If \( f : G \to \mathbb{C} \) is a complex-valued function on \( G \) and \( \chi : G \to \mathbb{C}^* \) is a character (group homomorphism) then we write
\[ c_\chi(f) = \frac{1}{p - 1} \sum_{h \in \hat{G}} f(h) \bar{\chi}(h) \]
for the corresponding Fourier coefficient of \( f \). We have
\[ f(v) = \sum_{\chi \in \hat{G}} c_\chi(f) \chi(v) \text{ where } \hat{G} = \text{Hom}(G, \mathbb{C}^*). \]

Let us consider the function
\[ d : G \to \mathbb{C}, \ d(v) = b'(v) - b(v). \]

What we need to check is that
\[ d(v) = d(-v) \forall v \in G, \]
which means that for all odd characters \( \chi \) (i.e., characters \( \chi \) of \( G \) with \( \chi(-1 \mod p) = -1 \))
the corresponding Fourier coefficient
\[ c_\chi(d) = 0. \]

It follows from (10) that \( d \ast j(-v) = 0 \) for all \( v \in G \), i.e.,
\[ d \ast j(v) = 0 \forall v \in G. \]

This implies that
\[ 0 = c_\chi(d \ast j) = c_\chi(d \cdot c_\chi(j)) \forall \chi \in \hat{G}. \]
However, \( c_\chi(j) \neq 0 \) for all odd \( \chi \): it follows from \([8\) Chap. 16, Theorem 2\] combined with \([7\) Ch. 9, p. 288, Th. 9.9\], see also \([13\) p. 477\]. This implies that \( c_\chi(d) = 0 \) for all odd \( \chi \). This ends the proof of the first assertion.

Now let \( p = 3 \). Then \( 2 + 2g/(p - 1) = g + 2 \) and \( G = \{1, -1\} \). We already know that

\[
b'(1) - b'(-1) = b(1) - b(-1).
\]

Now has only to recall that

\[
b'(1) + b'(-1) = g + 2 = b(1) + b(-1).
\]

\[\square\]

**Remark 1.14.** If \( v \in G \) then there is an integer \( k_v \) that does not divide \( p \) and such that \( j(vh) - kj(h) \) is divisible by \( p \) for all \( h \in G \). Indeed, the function

\[\gamma : G \to (\mathbb{Z}/p\mathbb{Z})^*, \ h = j \mod p \mapsto j(h) \mod p \]

is a group homomorphism. Hence,

\[\gamma(vh) = \gamma(v)\gamma(h) \ \forall v, h \in G.\]

Let us choose an integer \( k_v \in \mathbb{Z} \) such that

\[k_v \mod \mathbb{Z} = \gamma(h) = j(h) \mod \mathbb{Z}.\]

Clearly, \( p \) does not divide \( k_v \) and

\[j(vh) \mod p = \gamma(vh) = \gamma(v) \cdot \gamma(h) = (k_v \mod p) \cdot \gamma(h) = (k_v \mod p) \cdot (j(h) \mod p).\]

This implies that \( j(vh) - k_v j(h) \) is divisible by \( p \) for all \( v \in G \).

**Corollary 1.15.** Let \( c : G \to \mathbb{Z} \) be an integer-valued function. Then the following conditions are equivalent.

(i) \[c \ast h(1 \mod p) = \sum_{h \in G} c(h)j(h^{-1}) \in \mathbb{Z}.\]

(ii) \[c \ast h(h) = \sum_{h \in G} c(h)j(vh) \in \mathbb{Z} \ \forall v \in G.\]

**Proof.** Notice that in light of Remark 1.14 (applied to \( h^{-1} \)), if \( v \in G \) then there exists \( k_v \in \mathbb{Z} \) such that \( j(vh) - k_v j(h) \) is divisible by \( p \) for all \( h \in G \). In other words, \( j(v/h) = k_v j(h) \mod p \) and therefore

\[
\sum_{h \in G} c(h)j(v/h) \equiv k_v \sum_{h \in G} c(h)j(h^{-1}) \mod p \ \forall v \in G
\]

This ends the proof. \[\square\]

2. A CONSTRUCTION OF JACOBIANS

The following theorem may be viewed as an inverse of Theorem 1.14.

**Theorem 2.1.** Let \( g \) be a positive integer, \( p \) an odd prime, \( \zeta_p \in \mathbb{C} \) a primitive \( p \)th root of unity, and \( G = (\mathbb{Z}/p\mathbb{Z})^* \). Suppose that \( (p - 1) \) divides \( 2g \). Let \( \mathbf{b} : G \to \mathbb{Z}_+ \) be a non-negative integer-valued function such that

\[(i)\]

\[
\sum_{h \in G} \mathbf{b}(h) = \frac{2g}{p - 1} + 2.
\]
Let \( \{ f_h(x) \mid h \in G \} \) be a \((p-1)\)-element set of mutually prime nonzero polynomials \( f_h(x) \in \mathbb{C}[x] \) that enjoy the following properties.

1. \( \deg(f_h) = b(h) \) for all \( h \in G \). In particular, \( f_h(x) \) is a (nonzero) constant polynomial if and only if \( b(h) = 0 \).
2. Each \( f_h(x) \) has no repeated roots.

Let us consider a polynomial

\[
f(x) = f_b(x) = \prod_{h \in G} f_h(x)^{b(h)^{-1}} \in \mathbb{C}[x]
\]

of degree \( \sum_{h \in G} b(h)j(h^{-1}) \). Let \( \mathcal{C} \) be the smooth projective model of the irreducible plane affine curve

\[
y^2 = f_b(x)
\]

endowed with an automorphism \( \delta : \mathcal{C} \rightarrow \mathcal{C} \) induced by

\[
(x, y) \mapsto (x, \zeta_p y).
\]

Let \((J, \lambda)\) be the canonically principally polarized jacobian of \( \mathcal{C} \) endowed by the automorphism \( \delta \) induced by \( \delta_{CV} \). Then \( \mathcal{J} \) and \( \delta \) enjoy the following properties.

- (a) \( \dim(J) = g \)
- (b) \( \sum_{j=0}^{p-1} \delta^j = 0 \) in \( \text{End}(J) \).
- (c) \( \lambda \) is a (nonzero) constant

Let \( \alpha : G \rightarrow \mathbb{Z}_+ \) be the corresponding multiplicity function attached to the action of \( \delta \) on the differentials of first kind on \( X \) \((4)\). Then

\[
\alpha(v) = \frac{(p-1)}{p} \cdot b \ast j(-v) - 1 \quad \forall v \in G.
\]

Proof. If \( \alpha \) is a root of \( f(x) \) then there is exactly one \( h \in G \) that \( \alpha \) is a root of \( f_h(x) \); in addition, the multiplicity of \( \alpha \) (viewed as a root of \( f(x) \)) is \( j(h^{-1}) \), which is not divisible by \( p \). This implies that \( f(x) \) is not a \( p \)-th power in the polynomial ring \( \mathbb{C}[x] \) and even in the field of rational function \( \mathbb{C}(x) \). It follows from theorem 9.1 of \([4]\) Ch. VI, Sect. 9) that the polynomial \( y^p - f(x) \in \mathbb{C}(x)[y] \) is irreducible over \( \mathbb{C}[x] \). This implies that the polynomial in two variable \( y^p - f(x) \in \mathbb{C}[x, y] \) is irreducible, because every its divisor that is a polynomial in \( x \) is a constant. i.e., the affine plane curve \((24)\) is irreducible and its field of rational functions \( K \) is the field of fractions of the domain

\[
A = \mathbb{C}[x, y]/(y^p - f(x))\mathbb{C}[x, y].
\]

Let \( \mathcal{C} \) be the smooth projective model of \((24)\). Then \( K \) is the field \( \mathbb{C}(\mathcal{C}) \) of rational functions on \( \mathcal{C} \); in particular, \( \mathbb{C}(\mathcal{C}) \) is generated over \( \mathbb{C} \) by rational functions \( x, y \).

Let \( \pi : \mathcal{C} \rightarrow \mathbb{P}^1 \) be the regular map defined by rational function \( x \). Clearly, it has degree \( p \). Since

\[
\deg(\pi) = \deg(f) = \sum_{h \in G} b(h)j(h^{-1})
\]

is divisible by \( p \), the map \( \pi \) is unramified at \( \infty \) (see \([8]\) Sect. 4) and therefore the set of branch points of \( \pi \) coincides with the set of roots of \( f(x) \), which, in turn, is
the disjoint union of the sets $R_h$ of roots of $f_h(x)$. In particular, the number of
branch points of $\pi$ is

$$
\sum_{h \in G} \deg(f_h) = \sum_{h \in G} b(h) = \frac{2g}{p-1} + 2.
$$

Clearly, $\pi$ is a Galois cover of degree $p$, i.e., the field extension

$$
\mathbb{C}(C)/\mathbb{C}(\mathbb{P}^1) = \mathbb{C}(C)/\mathbb{C}(x)
$$

is a cyclic field extension of degree $p$. In addition, the cyclic Galois group
$\text{Gal}(\mathbb{C}(C)/\mathbb{C}(\mathbb{P}^1))$ is generated by the automorphism $\delta_C : C \to C$ induced by

$$
\delta_C : C \to C, \quad (x,y) \mapsto (x, \zeta_p y).
$$

It follows from the Riemann-Hurwitz formula (see [8, Sect. 4]) that the genus of $C$
is

$$
\frac{\left( \left( \frac{2g}{p-1} + 2 \right) - 2 \right) (p-1)}{2} = g.
$$

In addition, the automorphism $\delta$ of the polarized jacobian $(\mathcal{J}, \lambda)$ induced by $\delta_C$
satisfies the $p$th cyclotomic equation

$$
\sum_{j=0}^{p-1} \delta^j = 0 \quad \text{in} \quad \text{End}(\mathcal{J}).
$$

Let $B \subset C(\mathbb{C})$ be the set of ramification points of $\pi$. Clearly, $B$ coincides with the
set of fixed points of $\delta_C$. The map $x : C(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ establishes a bijection between $B$ and the disjoint union of all $R_h$’s. Let us put $B_h = \{ P \in B \mid x(P) \in R_h \}$.

Then $B$ partitions onto a disjoint union of all $B_h$’s and

$$
\#(B_h) = \deg(f_h) = b(h) \quad \forall h \in G.
$$

Let $P \in B$. The action of $\delta$ on the tangent space to $C$ at $P$ is multiplication by a
certain $p$th root of unity $\epsilon_P$. I claim that $\epsilon_P = \zeta_p^{j(h)}$ if $P \in R_h$.

Indeed, we have $x(P) = \alpha \in R_h$, $y(P) = 0$.

Let

$$
\text{ord}_P : \mathbb{C}(C) \to \mathbb{Z}
$$

be the discrete valuation map attached to $P$. Then one may easily check that

$$
\text{ord}_P(x - \alpha) = p, \quad \text{ord}_P(x - \beta) = 0 \quad \forall \beta \in \mathbb{C} \setminus \alpha.
$$

This implies that

$$
p \cdot j(h^{-1}) \cdot \text{ord}_P(x - \alpha) = \text{ord}_P(y^p) = p \cdot \text{ord}_P(y)
$$

and therefore

$$
\text{ord}_P(y) = j(h^{-1}).
$$

In light of [7], there is an integer $m$ such that $j(h^{-1}) \cdot j(h) = 1 + pm$. 

\begin{align*}
\text{ord}_P(y) &= j(h^{-1}) \\
\text{ord}_P(y^p) &= p \cdot \text{ord}_P(y) \\
\text{ord}_P(y) &= j(h^{-1}).
\end{align*}
Combining this with (25), we obtain that
\[
\text{ord}_\ell \left( \frac{g^{j(h)}}{(x - \alpha)^m} \right) = j(h^{-1}) \cdot j(h) - pm = 1
\]
and therefore \( t := g^{j(h)}/(x - \alpha)^m \) is a local parameter of \( C \) at \( P \). Clearly, the action of \( \delta \) multiplies \( t \) by \( \zeta_P^{j(h)} \) and therefore \( \epsilon_P = \zeta_P^{j(h)} \), which proves the Claim.

Now the desired result follows from Proposition 1.11 applied to \( X = J, \phi = \delta \).

**Example 2.2.** Let \( p = 3 \). The number of admissible functions is \((g + 1)\).

Let us list all the possibilities for \( a \) when \( g \) is given. Let us identify
\[
G = (\mathbb{Z}/3\mathbb{Z})^* = \{ 1 \text{ mod } 3, 2 \text{ mod } 3 \}
\]
with the set \( \{1, 2\} \) in the obvious way. We have the following conditions on \( b \).

\[ b(1), b(2) \in \mathbb{Z}_+, \quad b(1) + b(2) = g + 2, \quad 3 \mid (b(1) + 2b(2)). \]

The congruence condition means that \( b(1) \equiv b(2) \mod 3 \). So, the conditions on \( b \) are as follows.

\[ b(1), b(2) \in \mathbb{Z}_+, \quad b(1) + b(2) = g + 2, \quad b(1) \equiv b(2) \mod 3. \]

The list (and number) of corresponding \( a \) depends on \( g \mod 3 \). Namely, there are the natural three cases.

(i) \( g \equiv 1 \mod 3 \), i.e., \( g = 3k + 1 \) where \( k \) is a nonnegative integer. Then

\[ b(1) + b(2) = g + 2 = 3k + 3 = 3(k + 1), \]

and therefore both \( b(1) \) and \( b(2) \) are divisible by 3. Hence there are exactly \((k + 2)\) options for \( b \), namely,

\[ b(1) = 3d, \quad b(2) = 3(k + 1 - d); \quad d = 0, \ldots, (k + 1). \]

The corresponding \( a \) are as follows (where \( d = 0, \ldots, (k + 1) \)).

\[ a(2) = \frac{1}{3} (b(1) + 2b(2)) - 1 = d + 2(k + 1 - d) - 1 = d + 2(k + 1) - 1 = (2k + 1) - d; \]

\[ a(1) = \frac{1}{3} (2b(1) + b(2)) - 1 = 2d + (k + 1 - d) - 1 = k + d. \]

So, we get

\[ a(1) = k + d, \quad a(2) = (2k + 1) - d; \quad d = 0, \ldots, k + 1. \]

The number of \( a \)'s is

\[ k + 2 = \frac{g + 5}{3}. \]

(ii) \( g \equiv 2 \mod 3 \), i.e., \( g = 3k + 2 \) where \( k \) is a nonnegative integer. Then

\[ b(1) + b(2) = g + 2 = 3k + 4 = 3(k + 1) + 1, \]

and therefore both \( b(1) - 2 \) and \( b(2) - 2 \) are divisible by 3. Hence there are exactly \((k + 1)\) options for \( b \), namely,

\[ b(1) = 3d + 2, \quad b(2) = 3(k - d) + 2; \quad (d = 0, \ldots, k). \]

The corresponding \( a \) are as follows (where \( d = 0, \ldots, k \)).

\[ a(2) = \frac{1}{3} (b(1) + 2b(2)) - 1 = d + 2(k - d) + 2 - 1 = (2k + 1) - d; \]

\[ a(1) = \frac{1}{3} (2b(1) + b(2)) - 1 = 2d + (k - d) + 2 - 1 = (k + 1) + d = k + d. \]
So, we get

\begin{align}
\mathbf{a}(1) &= (k + 1) + d, \mathbf{a}(2) = (2k + 1) - d; \ d = 0, \ldots, k. \\
\end{align}

The number of \(a\)'s is

\[ k + 1 = \frac{g + 1}{3}. \]

(iii) \( g \equiv 0 \mod 3 \), i.e., \( g = 3k \) where \( k \) is a positive integer. Then

\[ \mathbf{b}(1) + \mathbf{b}(2) = g + 2 = 3k + 2, \]

and therefore both \( \mathbf{b}(1) - 1 \) and \( \mathbf{b}(2) - 1 \) are divisible by 3. Hence there are exactly \((k + 1)\) options for \(b\), namely,

\begin{align}
\mathbf{b}(1) &= 3d + 1, \mathbf{b}(2) = 3(k - d) + 1; \ (d = 0, \ldots, k). \\
The corresponding \(a\) are as follows (where \( d = 0, \ldots, k \)).
\end{align}

\begin{align}
\mathbf{a}(2) &= \frac{1}{3}(\mathbf{b}(1) + 2\mathbf{b}(2)) - 1 = d + 2(k - d) + 1 - 1 = 2k - d; \\
\mathbf{a}(1) &= \frac{1}{3}(2\mathbf{b}(1) + \mathbf{b}(2)) - 1 = 2d + (k - d) + 1 - 1 = k + d.
\end{align}

So, we get

\begin{align}
\mathbf{a}(1) &= k + d, \mathbf{a}(2) = 2k - d; \ d = 0, \ldots, k. \\
The number of \(a\)'s is
\end{align}

\[ k + 1 = \frac{g + 3}{3}. \]

\[ \square \]

References

[1] M. F. Atiyah, R. Bott, A Lefschetz fixed point formula for elliptic differential operators. Bull. Amer. Math. Soc. 72 (1966), 245–250.

[2] Ph. Griffiths, J. Harris, Principles of algebraic geometry. John Wiley and Sons, New York, 1978.

[3] K. Ireland, M. Rosen, A classical Introduction to Modern Number Theory, 2nd ed., Graduate Texts in Mathematics, Vol. 84, Corr. 5th printing, Springer-Verlag, New York, 1998.

[4] S. Lang, Algebra, Revised 3rd edition. Graduate Texts in Mathematics 211, Springer Science, 2002.

[5] J. Milnor, Dynamics in one complex variable. Vieweg, Braunschweig/Wiesbaden, 1999.

[6] B. Moonen, Yu.G. Zarhin, Weil classes on abelian varieties. J. reine angew. Math. 496 (1998), 83-92; Erratum https://www.math.ru.nl/~bmoonen/Papers/ErratumCrelle98.pdf.

[7] H. L. Montgomery, R. C. Vaughan, Multiplicative Number Theory. I. Classical Theory, Cambridge Tracts in Advanced Mathematics, Vol. 97, Cambridge University Press, Cambridge, 2007.

[8] B. Poonen, E. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line. J. Reine Angew. Math. 488 (1997), 141–188.

[9] K.A. Ribet, Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. 98 (1976), no. 3, 751–804.

[10] G. Shimura, Abelian varieties with complex multiplication and modular functions. Princeton University Press, Princeton, NJ, 1997.

[11] A. Weil, Zum Beweis des Torellischen Satzes. Göt. Nachr. 1957, no. 2, pp. 33–53; Œuvres, vol. III, [1957a].

[12] A. Weil, Sur le théorème de Torelli. Séminaire Bourbaki 151 (Mai 1957). Available at http://www.numdam.org/item/SC_1956-1958__4__207_0.pdf.

[13] J. Xue, Yu. G. Zarhin, Centers of Hodge groups of superelliptic jacobians. Transformation Groups 15 (2010), 449–482.
[14] Yu. G. Zarhin, *Cubic surfaces and cubic threefolds, jacobians and intermediate jacobians*. In: Algebra, Arithmetic and Geometry (Manin Festschrift). Progress in Math. 270, Birkhäuser, 2009, pp. 687–691.

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

Email address: zarhin@math.psu.edu