JOURNAL OF ALGEBRA 52, 378–410 (1978)

On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic $p > 2$

NORIKO YUI

Matematisk Institut, Københavns Universitet, Universitetsparken 5, 2100 København Ø, Denmark

Communicated by J. A. Dieudonné

Received October 15, 1977

1. INTRODUCTION

It is well known that an Abelian variety X of dimension g defined over a field k of characteristic $p > 0$ yields a p-divisible group $X(p)$ of dimension g and of height $2g$. Let $\mathbf{\Gamma}$ be the formal group obtained by expansion into power series of the group law of X relative to some system of local parameters at the origin. Then $\mathbf{\Gamma}$ is nothing but the connected p-divisible group in $X(p)$ and $\mathbf{\Gamma}$ has any height between g and $2g$ (cf. Tate [14]).

In the present paper, we confine ourselves to the study of the Jacobian variety $J(C)$ of a hyperelliptic curve C over a field of characteristic $p > 2$. Our aims here are (i) to determine the structures of the p-divisible group $J(p)$ and of the formal group $\mathbf{\Gamma}$ of $J(C)$ (up to isogeny) with the help of the Cartier–Manin matrix A of C, and (ii) to investigate how much information about the algebraic (global) structure of $J(C)$ (up to isogeny) can be recovered from the formal (local) structure.

We shall give a brief survey of the paper here. In Section 2, we define the Cartier–Manin matrix A of a hyperelliptic curve C over a perfect field of characteristic $p > 2$ following Cartier [1] and Manin [8]. We then show that A coincides with the Hasse–Witt matrix of C. Some basic but important properties of A are also discussed. After this, throughout the forthcoming sections, we assume that k is a finite field with p^a ($a \geqslant 1$) elements. In Section 3, we give a complete characterization of the "ordinary" Jacobian variety $J(C)$ of C. When $J(C)$ is ordinary, the Cartier–Manin matrix A of C completely determines the formal structure $J(p)$, and in certain cases the algebraic structure as well (up to isogeny). In the rest of the paper, we study the Jacobian variety $J(C)$ of the hyperelliptic curve C whose Cartier–Manin matrix has determinant zero in k. In Section 4, we observe that the Cartier–Manin matrix A of C no longer provides enough information; it is the p-adic exponents of the eigenvalues of the characteristic polynomial of the Frobenius endomorphism of $J(C)$ relative to k that determine

0021-8693/78/0522–0378$02.00/0

the isogeny class of $J(p)$. In Section 5, we characterize the "supersingular" Jacobian variety $J(C)$ of C. It is shown that, in this case, the formal group of $J(C)$ completely determines the algebraic structure of $J(C)$. We also show that the condition $A = (0)$ in k is sufficient but not necessary for $J(C)$ to be supersingular. In Section 6, we discuss the Jacobian variety $J(C)$ whose formal group Γ is isogenous to the symmetric formal group of dimension g. Finally, in Section 7, we consider the Jacobian variety $J(C)$ with the formal structure of the mixed type. It turns out that there is a k-simple Jacobian variety $J(C)$ with $J(p)$ isogenous to the mixed type $rG_{1,0} + (g - r)G_{1,1}$. We remark here that the Newton polygon $\mathfrak{N}(P_\pi)$ of the characteristic polynomial of the Frobenius endomorphism π of $J(C)$ relative to k, is a very useful tool for finding the local decomposition of $J(C)$ into isotypic (unfortunately not simple) components.

All formal groups and p-divisible groups discussed in this paper are commutative.

This paper is the result of my attempt to understand Manin's works [6, 7]. In the present paper, we deal only with the hyperelliptic curves, but we shall consider more general cases (algebraic curves) in the forthcoming paper [16].

2. The Cartier–Manin Matrix of a Hyperelliptic Curve over a Perfect Field of Characteristic $p > 2$

Let k be a perfect field of characteristic $p > 2$ and let C be a complete non-singular curve over k defined by the equation

$$C : y^2 = f(x), \tag{1}$$

where $f(x)$ is a polynomial over k without multiple roots of degree $2g + 1$.

Denote by $K = k(x, y)$ the algebraic function field of C of one variable over k. Then K has the unique subfield $K^p = k^p(x^p, y^p) = k(x^p, y^p)$ over which K is separably generated, e.g., $K = K^p(x)$ for a separably generating transcendental element $x \in K - K^p$. Let $\Omega^1(K)$ be the space of all differential forms of degree 1 on K and $d : K \to \Omega^1(K)$ the canonical derivation of K. Since $dx \neq 0$ for a separating element x, every element $\omega \in \Omega^1(K)$ can be expressed uniquely in the form

$$\omega = d\phi + \psi^p\, dx/x \qquad \text{with} \quad \phi, \psi \in K,\ \psi^p \in K^p. \tag{2}$$

Definition 2.1. Let $\Omega^1(K^p)$ be the space of all differential forms of degree 1 on K^p and $d^p : K^p \to \Omega^1(K^p)$ the corresponding derivation of K^p to d. We define *the Cartier operator* $\mathscr{C} : \Omega^1(K) \to \Omega^1(K^p)$ by letting, for ω given as (2),

$$\mathscr{C}(\omega) = \psi^p(d^p x^p/x^p).$$

$\mathscr{C}$ is a well-defined K^p-linear operator and $\mathscr{C}(d\phi) = 0$.

Sometimes it is convenient to use the following expression for $\omega \in \Omega^1(K)$:

$$\omega = d\phi + \eta^p x^{p-1}\, dx \qquad \text{with} \quad \phi, \eta \in K, \eta^p \in K^p. \tag{2'}$$

Definition 2.1′. *The modified Cartier operator* $\mathscr{C}' : \Omega^1(K) \to \Omega^1(K)$ is defined for ω given as (2′) by

$$\mathscr{C}'(\omega) = \eta\, dx.$$

Proposition 2.1. *The basic properties of the modified Cartier operator $\mathscr{C}'$ are summarized as follows:*

(a) $\mathscr{C}'(\omega + \omega') = \mathscr{C}'(\omega) + \mathscr{C}'(\omega')$.

(b) $\mathscr{C}'(\phi^p \omega) = \phi \mathscr{C}'(\omega)$ *for* $\phi \in K$.

(c) $\mathscr{C}'(\phi^{n-1}\, d\phi) = d\phi$ *if* $n = p$, *and* 0 *otherwise, for* $\phi \in K$.

(d) $\mathscr{C}'(\omega) = 0 \Leftrightarrow \omega = d\phi$ *with some* $\phi \in K$.

If this is the case, ω *is called exact.*

(e) $\mathscr{C}'(\omega) = \omega \Leftrightarrow \omega = d\phi/\phi$ *with some* $\phi \in K$.

If this is the case, ω *is called logarithmic.*

Proof. They are immediately derived from the definition except (e). For (e) see Cartier [1]. Q.E.D.

Now the differential forms of degree 1 and of the first kind on K form a k-vector space, denoted, $\mathfrak{D}_0(K)$, of dimension g with a system of the canonical basis

$$\mathscr{B} = \left\{\omega_i = \frac{x^{i-1}\, dx}{y}, i = 1,..., g\right\}. \tag{3}$$

The images of the ω_i's under the modified Cartier operator $\mathscr{C}'$ are determined in the following way due to Manin [8]. Rewrite ω_i as

$$\omega_i = \frac{x^{i-1}\, dx}{y} = x^{i-1} y^{-p} y^{p-1}\, dx = y^{-p} x^{i-1} \sum_{j=0}^{N} c_j x^j\, dx,$$

where the coefficients $c_j \in k$ are obtained from the expansion

$$f(x)^{(p-1)/2} = \sum_{j=0}^{N} c_j x^j, \qquad N = \frac{p-1}{2}(2g+1).$$

Then we get for $i = 1,\dots, g$,

$$\omega_i = y^{-p}\Bigl(\sum_{\substack{j\\ i+j\not\equiv 0\ (\mathrm{mod}\, p)}} c_j x^{j+i-1}\, dx\Bigr) + \sum_l c_{(l+1)p-i}\,\frac{x^{(l+1)p}}{y^p}\,\frac{dx}{x}$$

$$= d\Bigl(y^{-p}\sum_{\substack{j\\ i+j\not\equiv 0\ (\mathrm{mod}\, p)}} \frac{c_j x^{j+i}}{j+i}\Bigr) + \sum_l c_{(l+1)p-i}\,\frac{x^{lp}}{y^p}\,x^{p-1}\, dx.$$

Note here that

$$0 \leqslant l \leqslant \frac{N+i}{p} - 1 = \frac{((p-1)/2)(2g+1)+i}{p} - 1 < g - \frac{1}{2}.$$

Thus we have

$$\mathscr{C}'(\omega_i) = \sum_{l=0}^{g-1} c^{1/p}_{(l+1)p-i}\,\frac{x^l}{y}\, dx.$$

This shows that $\mathfrak{D}_0(K)$ is closed under the modified Cartier operator $\mathscr{C}'$. Thus we can represent $\mathscr{C}'$ by a matrix. Indeed, if we write $\boldsymbol{\omega} = (\omega_1,\dots,\omega_g)$, we have

$$\mathscr{C}'(\boldsymbol{\omega}) = A^{(1/p)}\boldsymbol{\omega},$$

where A is the $(g \times g)$ matrix with elements in k given as

$$A = \begin{pmatrix} c_{p-1} & c_{p-2} & \cdots & c_{p-g} \\ c_{2p-1} & c_{2p-2} & \cdots & c_{2p-g} \\ & \cdots & & \\ c_{gp-1} & c_{gp-2} & \cdots & c_{gp-g} \end{pmatrix}.$$

(Correspondingly, under the Cartier operator $\mathscr{C}$, we have

$$\mathscr{C}(\omega_i) = \sum_{l=0}^{g-1} c_{(l+1)p-i}\,\frac{x^{(l+1)p}}{y^p}\,\frac{d^p x^p}{x^p}$$

and hence

$$\mathscr{C}(\boldsymbol{\omega}) = A\boldsymbol{\omega}^p.)$$

DEFINITION 2.2. The matrix A obtained above is called *the Cartier–Manin matrix* of the hyperelliptic curve C of genus g defined over k (with respect to the canonical basis $\boldsymbol{\omega}$ of $\mathfrak{D}_0(K)$). We denote it by $H(C, \boldsymbol{\omega})$.

PROPOSITION 2.2. *The Cartier–Manin matrix A of C is determined up to transformation of the form $S^{(p)}AS^{-1}$, where $S = (s_{ij})$, $s_{ij} \in k$ is a $(g \times g)$ non-singular matrix and $S^{(p)} = (s_{ij}^p)$, independently of the choice of the basis of $\mathfrak{D}_0(K)$.*

Proof. Let $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_g)$ be any system of the first kind of differential forms of degree 1 on K. Then there exists a $(g \times g)$ nonsingular matrix $S = (s_{ij})$ with elements in k such that

$$\theta_i = \sum_{j=1}^{g} s_{ij}\omega_j \qquad (i = 1, \ldots, g),$$

and there is a commutative diagram

$$\begin{array}{ccc} \boldsymbol{\omega} = (\omega_1, \ldots, \omega_g) & \xrightarrow{\mathscr{C}} & H(C, \boldsymbol{\omega})\boldsymbol{\omega}^p \\ {\scriptstyle S}\big\downarrow & & \big\downarrow{\scriptstyle S^{(p)}} \\ \boldsymbol{\theta} = (\theta_1, \ldots, \theta_g) & \xrightarrow{\mathscr{C}} & H(C, \boldsymbol{\theta})\boldsymbol{\theta}^p \end{array}$$

Hence A is transformed to $S^{(p)} AS^{-1}$. This shows that A is determined up to transformation of the form $S^{(p)} AS^{-1}$ independently of the choice of the basis of $\mathfrak{D}_0(K)$. Q.E.D.

THEOREM 2.1. *Assume that k is algebraically closed. Let $A = H(C, \boldsymbol{\omega})$ be the Cartier–Manin matrix of the hyperelliptic curve C over k of genus g, with respect to the canonical basis $\boldsymbol{\omega}$ of $\mathfrak{D}_0(K)$ given as* (3). *Denote by $\mathbf{a} = {}^t(a_1, \ldots, a_g)$ a g-column vector with elements in k and let us put*

$$H = \{\mathbf{a}\boldsymbol{\omega} \in \mathfrak{D}_0(K) \mid A\, A^{(p)} \cdots A^{(p^{g-1})}\mathbf{a}^{p^g} = \mathbf{0}\}$$

and

$$G = \{\mathbf{a}\boldsymbol{\omega} \in \mathfrak{D}_0(K) \mid A\, \mathbf{a}^p = \mathbf{a}\}.$$

Suppose that the matrix $A\ A^{(p)} \cdots A^{(p^{g-1})}$ has rank r. *Then H is a k-vector subspace of $\mathfrak{D}_0(K)$ of dimension $g - r$ and G generates a k-vector subspace $[G]$ of dimension r. Moreover, $\mathfrak{D}_0(K)$ is isomorphic to a direct sum of H and $[G]$.*

Proof. Let us denote by

$$M = \{\mathbf{a} = {}^t(a_1, \ldots, a_g),\ a_i \in k \text{ for every } i\}$$

the set of all g-column vectors with elements in k. Then M becomes a $k[\mathscr{C}]$-module of rank g over k by defining the operation $\mathscr{C}\mathbf{a} = A\, a^p$ and $\mathscr{C}\alpha = \alpha^p\mathscr{C}$ for $\alpha \in k$. Put

$$M_1 = \{\mathbf{a} \in M \mid \mathscr{C}^g\mathbf{a} = A\, A^{(p)} \cdots A^{(p^{g-1})}\mathbf{a}^{p^g} = \mathbf{0}\}$$

and

$$M_2 = \{\mathbf{a} \in M \mid \mathscr{C}\mathbf{a} = A\, a^p = \mathbf{a}\}.$$

Suppose now that the matrix $A\ A^{(p)} \cdots A^{(p^{g-1})}$ has rank r. Then it is easy to see that M_1 is a $k[\mathscr{C}]$-submodule of M of rank $g - r$ over k. While M_2 itself is not a k-module (because $\mathscr{C}(\alpha\mathbf{a}) = A(\alpha\mathbf{a})^p = \alpha^p A\ a^p = \alpha^p\ \mathbf{a} \neq \alpha\mathbf{a}$ for $\alpha \in k$), but it generates a $k[\mathscr{C}]$-submodule $[M_2]$ of M of rank t, say over k. So there exists a system of k-basis $\{\mathbf{a}_1, \ldots, \mathbf{a}_t\}$ of $[M_2]$ which consists of the solutions of the equation $\mathscr{C}\mathbf{a} = A\ \mathbf{a}^p = \mathbf{a}$. Now an element $\sum_{i=1}^t \alpha_i\mathbf{a}_i \in [M_2]$ is the solution of the equation $\mathscr{C}\mathbf{a} = \mathbf{a}$, if and only if $\mathscr{C}(\sum_{i=1}^t \alpha_i\mathbf{a}_i) = \sum_{i=1}^t \alpha_i{}^p\mathbf{a}_i = \sum_{i=1}^t \alpha_i\mathbf{a}_i$, if and only if α_i are elements of the prime field $\mathbb{F}_p$ of characteristic $p > 0$. Therefore there are p^t solutions for $A\ \mathbf{a}^p = \mathbf{a}$ in M and we have

$$[M_2] = \left\langle \sum_{i=1}^{t} \alpha_i\mathbf{a}_i \mid \alpha_i \in \mathbb{F}_p \text{ and } \mathbf{a}_i \in M_2 \right\rangle.$$

It is easy to see that $M_1 \cap [M_2] = \{0\}$ and $M \supseteq M_1 \oplus [M_2]$.

Now we claim that $t = r =$ the rank of the matrix $A\ A^{(p)} \cdots A^{(p^{g-1})}$, whence $M = M_1 \oplus [M_2]$. For this take an arbitrary element $\mathbf{a}_0$ of M and let $k[\mathscr{C}]\mathbf{a}_0$ be the principal module generated over k by $\mathbf{a}_0, \mathscr{C}\mathbf{a}_0, \mathscr{C}^2\mathbf{a}_0, \ldots$. $k[\mathscr{C}]\mathbf{a}_0$ is finite dimensional over k, say of rank g_0, where g_0 is the degree of the minimal polynomial $P(X)$ of $\mathscr{C}$ over k:

$$P(\mathscr{C}) = \beta_{g_0}\mathscr{C}^{g_0} + \cdots + \beta_i\mathscr{C}^i + \cdots + \beta_0 = 0, \qquad \beta_i \in k.$$

Then $\mathbf{a}_0, \mathscr{C}\mathbf{a}_0, \ldots, \mathscr{C}^{g_0-1}\mathbf{a}_0$ constitute a system of k-basis for $k[\mathscr{C}]\mathbf{a}_0$, with $g_0 \leqslant g$.

Now we put $M_1{}^0 = \{\mathbf{b} \in k[\mathscr{C}]\mathbf{a}_0 \mid \mathscr{C}^{g_0}\mathbf{b} = \mathbf{0}\}$. Then $M_1{}^0$ is a $k[\mathscr{C}]$-submodule of $k[\mathscr{C}]\mathbf{a}_0$ of finite rank, say t_0 over k. Denote by $[M_2{}^0]$ the $k[\mathscr{C}]$-submodule of $k[\mathscr{C}]\mathbf{a}_0$ generated by the solutions of the equations $\mathscr{C}\mathbf{b} = \mathbf{b}$ in $k[\mathscr{C}]\mathbf{a}_0$, with finite rank, say s_0 over k. Then we have $g_0 \geqslant t_0 + s_0$.

Suppose now that β_{n_0} is the coefficient of $P(X)$ such that $\beta_{n_0} \neq 0$ for n_0 the smallest index with this property. Put

$$\phi_i(\lambda) = \beta_i\lambda + \beta_{i-1}^p\lambda^p + \cdots + \beta_0^{p^i}\lambda^{p^i}, \qquad i = 0, \ldots, g_0.$$

Then, k being algebraically closed, we see that

$$\phi_{g_0}(\lambda) = \beta_{g_0}\lambda + \beta_{g_0-1}^p\lambda^p + \cdots + \beta_{n_0}^{p^{g_0-n_0}}\lambda^{p^{g_0-n_0}}$$

has $p^{g_0-n_0}$ solutions in k. While, by noting that $\mathscr{C}\beta_i = \beta_i{}^p\mathscr{C}$, we have

$$(1 - \mathscr{C})\left(\sum_{i=0}^{g_0-1} \phi_i(\lambda)\,\mathscr{C}^i\right) + \phi_{g_0}(\lambda)\,\mathscr{C}^{g_0} = \lambda P(\mathscr{C}) = 0.$$

Hence we see that $(1 - \mathscr{C})\mathbf{b} = \mathbf{0}$, i.e., $\mathscr{C}\mathbf{b} = \mathbf{b}$ has $p^{g_0-n_0}$ solutions in $k[\mathscr{C}]\mathbf{a}_0$.

This implies that $s_0 \geqslant g_0 - n_0$. This together with the inequality $g_0 \geqslant s_0 + t_0$ gives $n_0 \geqslant t_0$. On the other hand, we have

$$0 = P(\mathscr{C}) = \mathscr{C}^{n_0} Q(\mathscr{C}) \qquad \text{with} \quad Q(\mathscr{C}) = \sum_{i=0}^{g_0 - n_0} \beta_{n_0+i}^{1/p^{n_0}} \mathscr{C}^i.$$

Then $Q(\mathscr{C})\mathbf{a}_0$, $\mathscr{C}Q(\mathscr{C})\mathbf{a}_0, \ldots, \mathscr{C}^{n_0-1}Q(\mathscr{C})\mathbf{a}_0$ are linearly independent elements of $M_1{}^0$. So $t_0 \geqslant n_0$. Therefore $t_0 = n_0$ and $k[\mathscr{C}]\mathbf{a}_0 = M_1{}^0 \oplus [M_2{}^0]$.

$\mathbf{a}_0$ being an arbitrary element of M and M_1 and $[M_2]$ being $k[\mathscr{C}]$-modules, the assertion $t = r$ follows from

$$\mathbf{a}_0 \in k[\mathscr{C}]\mathbf{a}_0 = M_1{}^0 \oplus [M_2{}^0] \subseteq M_1 \oplus [M_2].$$

The assertions of the theorem are immediately derived from the above discussion. In fact, H (resp. G) is canonically isomorphic as a group to M_1 (resp. M_2) and H becomes a k-vector subspace of $\mathfrak{D}_0(K)$ of dimension $g - r$, while G generates a k-vector subspace $[G]$ of $\mathfrak{D}_0(K)$ of dimension r. Q.E.D.

THEOREM 2.2. *Assume that k is algebraically closed. Let G and r be as in Theorem 2.1. Then G is canonically isomorphic to the group of classes of divisors of order p of K. In other words, the number of divisor classes of order p of K is precisely p^r.*

Proof. By Artin–Schreier theory, a cyclic extension of K of degree p can be obtained by adjoining a root $\mathscr{P}^{-1}z$ of the polynomial $\mathscr{P}X - z = 0$, $z \in K$ and $\mathscr{P}X = X^p - X$. Put $Z = K(\mathscr{P}^{-1}z)$. Then Z is unramified over K, if and only if Z is unramified at every place P of K, if and only if $z \in \mathscr{P} K_P$ for every P, where K_P denotes the completion of K at P, if and only if $z \in \mathscr{P}k((u_P))$ for every P, where $k((u_P))$ is the power series field over K in a local parameter u_P, if and only if $z \in U/\mathscr{P}K$ where $U = \bigcap_P (\mathscr{P}K_P \cap K)$ (note that $z \in \mathscr{P}K \Leftrightarrow Z = K$). Furthermore, we have the following lemmas.

LEMMA A. *Let $z \in U/\mathscr{P}K$ be as above. Then*

$$z \in \prod_{j=1}^{g} \left(\mathscr{L}\left(p \sum_{i=1}^{g} P_i\right) \cap \mathscr{P}K_{P_j}\right)\Big/k,$$

where $\{P_1, \ldots, P_g\}$ is a set of distinct k-rational points on C such that the divisor $\sum_{i=1}^g P_i$ is nonspecial and $\mathscr{L}(p \sum_{i=1}^g P_i)$ is the k-vector space of functions $0 \neq \xi \in K$ such that the divisor $(\xi) \geqslant -p \sum_{i=1}^g P_i$.

Proof of Lemma A. There exists a nonspecial system of points P_i, $i = 1, \ldots, g$, on C, corresponding to the first kind differentials ω_i, $i = 1, \ldots, g$, in K in the following way. Let $0 \neq \omega_1 \in \mathfrak{D}_0(K)$ and P_1 be a point which is not a zero of ω_1. Now the Riemann–Roch theorem says that the space of the first kind differentials having zero at P_1 has dimension $g - 1$. Let $0 \neq \omega_2 \in \mathfrak{D}_0(K)$ be in it and let P_2 be a point which is not a zero of ω_2. Continuing this process g times to get g points $P_1, \ldots, P_g$ with the index of speciality $i(\sum_{i=1}^{g} P_i) = l(\sum_{i=1}^{g} P_i) - d(\sum_{i=1}^{g} P_i) - g + 1 = 1 - g + g - 1 = 0$ where $l =$ dimension and $d =$ degree of $\mathscr{L}\left(\sum_{i=1}^{g}\right) P_i)$.

Now if an element $z \in K$ is integral at $P \neq P_i$, $i = 1, \ldots, g$, then a root α of the polynomial $f(X) = X^p - X - z = 0$ is integral at the place P' over P in $Z = K(\alpha)$ (because $\nu_{P'}(\alpha) \geqslant 0$ if and only if $\nu_P(\mathrm{Norm}_{Z/K}(\alpha)) = \nu_P(-z) \geqslant 0)$. So $\{1, \alpha, \ldots, \alpha^{p-1}\}$ is an integral basis of Z at P. Moreover, α is unramified at P, since the differential exponent is $\nu_{P'}(f'(\alpha)) = \nu_{P'}(-1) = 0$. This shows that

$$\mathscr{L}\left(p \sum_{i=1}^{g} P_i\right) \cap \mathscr{P}K_{P_j} \subseteq U \qquad \text{for} \quad i = 1, \ldots, g.$$

If $z \in \mathscr{L}(p \sum_{i=1}^{g} P_i) \cap \mathscr{P}K$, then there is $X \in K$ such that $z = X^p - X$. Hence X is integral for all $P \neq P_i$, $i = 1, \ldots, g$ and at P_i, X has a pole of order at most 1. Thus X is constant and so is z. So we have the injection

$$\prod_{j=1}^{g} \left(\mathscr{L}\left(p \sum_{i=1}^{g} P_i\right) \cap \mathscr{P}K_{P_j}\right) \Big/ k \rightarrowtail U/\mathscr{P}K.$$

Finally, we want to show that for a given $z \in U$, there exist $(z_1, \ldots, z_g)$, $z_j \in \mathscr{L}(p \sum_{i=1}^{g} P_i) \cap \mathscr{P}K_{P_j}$ such that $z \equiv (z_1, \ldots, z_g) \pmod{\mathscr{P}K}$. Let $z \in U = \bigcap_P (\mathscr{P}K_P \cap K)$. Suppose that z is not integral at $P \neq P_i$, $i = 1, \ldots, g$, then z has a pole at P of order pm with some positive integer $m \geqslant 1$ and z has a power series expansion by a local parameter u_P as $z \equiv (a/u_P^{pm}) \pmod{1/u_P^{pm-1}}$ with $a \in k$. Now by applying the Riemann–Roch theorem, there exists $w_1 \in \mathscr{L}(mP + \sum_{i=1}^{g} P_i)$ (whose dimension is $1 + m$) such that $w_1 \equiv (a^{1/p}/u_P{}^m) \pmod{1/u_P^{m-1}}$. Hence we see that $z \equiv \mathscr{P}w_1 \pmod{1/u_P^{pm-1}}$ and $z - \mathscr{P}w_1$ has a pole of smaller order than that of z at P. Repeating this procedure, we may assume, without loss of generality, that z has poles only at P_i, $i = 1, \ldots, g$. Hence $z \in \mathscr{P}K_{P_j} \cap K$, $j = 1, \ldots, g$. Now we must show that $z \in \mathscr{L}\ (p \sum_{i=1}^{g} P_i)$. Since $z \in \mathscr{P}K_{P_j} \cap K$, z has an expansion of the form by the local parameter u_{P_j} at $P_j : z \equiv (a_j/u_{P_j}^{pm_j}) \pmod{1/u_{P_j}^{pm_j-1}}$ with some integer $m_j \geqslant 1$ and $a_j \in k$. If $m_j = 1$ for every $j = 1, \ldots, g$, then $z \in \mathscr{L}(p \sum_{i=1}^{g} P_i)$. If $m_j > 1$, again by the Riemann–Roch theorem, there exists $w_j \in \mathscr{L}(m_j P_j)$ such that $w_j \equiv (a_j^{1/p}/u_{P_j}^{m_j}) \pmod{1/u_{P_j}^{m_j-1}}$. Hence $z - \mathscr{P}w_j$ has a pole of smaller order than that of z at P_j. Continuing this process, we finally get $z_j \in \mathscr{L}\ (p \sum_{i=1}^{g} P_i) \cap \mathscr{P}K_{P_j}$ for each $j = 1, \ldots, g$ with the required property and hence $z \in \mathscr{L}\ (p \sum_{i=1}^{g} P_i)$. Q.E.D.

An immediate consequence of Lemma A is that we have

$$z \equiv \frac{b_i{}^p}{u_{P_i}^p} - \frac{b_i}{u_{P_i}} \pmod{u_{P_i}^0} \qquad \text{with} \quad b_i \in k \quad \text{for} \quad i = 1, \ldots, g.$$

If we write $\mathbf{u} = (u_{P_1}, \ldots, u_{P_g})$ and $\mathbf{b} = (b_1, \ldots, b_g)$, we have

$$z \equiv \frac{\mathbf{b}^p}{\mathbf{u}^p} - \frac{\mathbf{b}}{\mathbf{u}} \pmod{u^0}.$$

LEMMA B. [2, Staz 4]. *Let P_i, $i = 1, \ldots, g$ be a nonspecial system of points on C and u_{P_i} a local parameter at P_i (taken as same as in Lemma* A). *Then there exist functions $v_j \in \mathscr{L}(p \sum_{i=1}^{g} P_i)$, $j = 1, \ldots, g$ such that*

$$v_j \equiv \frac{e_{ij}}{u_{P_i}^p} - \frac{d_{ij}}{u_{P_i}} \pmod{u_{P_i}^0},$$

where $e_{ij} = 1$ if $i = j$ and 0 otherwise and $d_{ij} \in k$. If we write $\mathfrak{v} = (v_1, \ldots, v_g)$, $I = (e_{ij})$, and $D = (d_{ij})$, we have

$$\mathfrak{v} \equiv \frac{I}{\mathbf{u}^p} - \frac{D}{\mathbf{u}} \pmod{u^0}.$$

DEFINITION 2.3. The matrix D obtained in Lemma B is called *the Hasse–Witt matrix* of the hyperelliptic curve C (cf. [2]).

LEMMA C [2, Hauptstaz]. *Let z be as in Lemma* A *and $\mathfrak{v}$ as in Lemma* B. *Then z* (mod k) *is in one-to-one correspondence with the vectors $\mathbf{b} = (b_1, \ldots, b_g)$, $b_i \in k$ for all i, satisfying $D\,\mathbf{b}^p = \mathbf{b}$ modulo multiplication by elements in the prime field of characteristic $p > 0$.*

LEMMA D. *The Hasse–Witt matrix D obtained in Lemma B is identified with the Cartier–Manin matrix A. Moreover, the group*

$$\{\mathbf{b} = (b_1, \ldots, b_g),\ b_i \in k \text{ for all } i \mid D\mathbf{b}^p = \mathbf{b}\}$$

is canonically isomorphic to G in Theorem 2.1.

Proof of Lemma D. Let $\mathfrak{A}$ be the space of adeles $\xi = (\cdots \xi_P \cdots)$ in K. For a divisor X in K, we denote by $\mathfrak{A}(X)$ the k-vector space $\{\xi \in \mathfrak{A} \mid \nu_P(\xi) \geqslant -\nu_P(X)$ for all $P\}$. Then we see that $\dim_k(\mathfrak{A}/(\mathfrak{A}(X) + K)) =$ the index of speciality of X. In particular, take $X = \sum_{i=1}^{k} P_i$: the nonspecial divisor. Then $\mathfrak{A} = \mathfrak{A}(\sum_{i=1}^{k} P_i) + K$ and the factor space $\mathfrak{A}/(\mathfrak{A}(0) + K)$ is generated by the adeles $\xi_i = (\cdots 1/u_{P_i} \cdots)$ and $(\xi_1, \ldots, \xi_g)$ is the canonical basis for $\mathfrak{A}/(\mathfrak{A}(0) + K)$. The k-vector spaces $\mathfrak{D}_0(K)$ and $\mathfrak{A}/(\mathfrak{A}(0) + K)$ are dual and there is a pairing between them given in the following fashion. Let W be the canonical divisor. Then there is a sequence of k-vector spaces:

$$\mathscr{L}\left(W - \sum_{i=1}^{g} P_i\right) \subseteq \mathscr{L}\left(W - \sum_{i=1}^{g-1} P_i\right) \subseteq \cdots \subseteq \mathscr{L}\left(W - \sum_{i=1}^{j} P_i\right)$$

$$\subseteq \mathscr{L}\left(W - \sum_{i=1}^{j-1} P_i\right) \subseteq \cdots \subseteq \mathscr{L}(W - P_1) \subseteq \mathscr{L}(W)$$

$$\text{with} \quad l\left(W - \sum_{i=1}^{j-1} P_i\right) - l\left(W - \sum_{i=1}^{j} P_i\right) = 1.$$

Hence it follows from the choice of P_i and from the Riemann–Roch Theorem that

$$\omega_j \in \Omega\left(\sum_{i=1}^{j-1} P_i\right) \setminus \Omega\left(\sum_{i=1}^{j} P_i\right) \qquad \text{for each} \quad 1 \leqslant j \leqslant g,$$

where $\Omega(X) = \{\omega \in \Omega^1(K) | (\omega) \geqslant X\}$ and that $(\omega_1, ..., \omega_g)$ is a dual basis to $(\xi_1, ..., \xi_g)$.

Now let S be the matrix of scalars $(\omega_i, \xi_j) =:$ the residue of $\omega_i \xi_j$ at P_j. We may take S to be the $(g \times g)$ identity matrix by identifying the local parameters u_{P_i} with x^i/y for $i = 1, ..., g$ (note that x^i/y, $i = 1, ..., g$ can be local parameters, since $\omega_i = (x^{i-1}/y)\, dx$, $i = 1, ..., g$ are linearly independent). Hence we get

$$((\omega_i, \xi_j^p)) = ((\mathscr{C}\omega_i, \xi_j)^p) = A.$$

While we have for the functions v_j, $j = 1, ..., g$ in Lemma B,

$$(\mathbf{0}) = ((\omega_i, v_j)) = ((\omega_i, \xi_j^p)) - D((\omega_i, \xi_j)) = A - D.$$

Hence $A = D$ and the group $\{\mathbf{b} = (b_1, ..., b_g),\ b_i \in k$ for all i satisfying $D\, \mathbf{b}^p = \mathbf{b}\}$ is canonically isomorphic to G. Q.E.D.

LEMMA E. *The number of classes of divisors of order p of K is precisely p^r where r is the rank of the matrix $A\, A^{(p)} \cdots A^{(p^{g-1})}$.*

Proof of Lemma E. As an immediate consequence of Lemma D and of Theorem 2.1, we know that there are p^r solutions for the system of equations $D\, \mathbf{b}^p = \mathbf{b}$ in k. Hence there are p^r divisor classes of order p of K. Q.E.D.

This completes the proof of Theorem 2.2. Q.E.D.

COROLLARY 2.3. *The notations and the hypothesis being as in Theorems* 2.1 *and* 2.2, *we have*

(a) *The following statements are equivalent*:

(ai) $r = g$.

(aii) $|A\, A^{(p)} \cdots A^{(p^{g-1})}| \neq 0$.

(aiii) *A has rank g.*

(aiv) $\mathfrak{D}_0(K)$ *does not posess any exact differentials.*

(b) *All differentials of* $\mathfrak{D}_0(K)$ *are exact, if and only if* $A = (0)$. *When this is the case,* $A\ A^{(p)} \cdots A^{(p^{g-1})}$ *has rank 0 and there are no classes of divisors of order p of K*

Proof. (a) (ai) $\Leftrightarrow$ (aii) $\Leftrightarrow$ (aiii) are clear, since determinant is multiplicative. (ai) $\Leftrightarrow$ (aiv). Suppose (ai), then $\mathfrak{D}_0(K) = [G]$ and $\mathscr{C}\boldsymbol{\theta} = \boldsymbol{\theta}$ for every $\boldsymbol{\theta} \in \mathfrak{D}_0(K)$, whence (aiv). The converse is clear.

(b) The equivalence follows from the definition of A and from Theorem 2.1. The last assertion is a trivial consequence of Theorem 2.2. Q.E.D.

3. Ordinary Jacobian Variety $J(C)$ of C

From here on, let k be a finite field of characteristic $p > 2$ *with* p^a $(a \geq 1)$ *elements and* $\bar{k}$ *its algebraic closure.*

Let C be the hyperelliptic curve defined over k by the equation (1) and $J(C)$ its Jacobian variety. We may assume that $J(C)$ and its canonical embedding $C \to J(C)$ are also defined over k. Let π be the Frobenius endomorphism of $J(C)$ relative to k with the characteristic polynomial $P_\pi(\lambda) \in \mathbb{Z}[\lambda]$ of degree $2g$. $P_\pi(\lambda) = \sum_{i=0}^{2g} a_i\lambda^i$, $a_0 = p^{ag}$, $a_{2g} = 1$. $P_\pi(\lambda)$ is the characteristic polynomial of the l-adic and also of the p-adic representation of the Frobenius endomorphism π and it is of special interest, because (1) it determines the isogeny class of $J(C)$ [13] and (2) the p-adic values of its characteristic roots determine the formal structure of $J(C)$ up to isogeny [6]. Thus $P_\pi(\lambda)$ determines the formal and algebraic structure of $J(C)$ up to isogeny.

Henceforth, there remains the main task of determining $P_\pi(\lambda)$ explicitly. Its dependence on the Cartier–Manin matrix A of C has been illuminated by Manin [7]. That is, $P_\pi(\lambda)$ is linked to the Cartier–Manin matrix through the congruence

$$P_\pi(\lambda) \equiv (-1)^g \lambda^g \mid A_\pi - \lambda I_g \mid \qquad (\mathrm{mod}\ p), \tag{4}$$

where $\mid A_\pi - \lambda I_g \mid$ is the characteristic polynomial of the matrix $A_\pi = A\ A^{(p)} \cdots A^{(p^{a-1})}$ and I_g is the $(g \times g)$ identity matrix.

Theorem 3.1. *Let C be the hyperelliptic curve of genus g defined by* (1) *over k: a finite field of* p^a $(a \geqslant 1)$ *elements,* $p > 2$ *and* $J(C)$ *its Jacobian variety defined over k. Let* π *be the Frobenius endomorphism of* $J(C)$ *relative to k and* $P_\pi(\lambda)$ *its characteristic polynomial. Then the following statements are equivalent:*

(i) $\mid A_\pi \mid \neq 0$.

(ii) *A has rank g, i.e.,* $\mid A \mid \neq 0$.

(iii) *$A\,A^{(p)} \cdots A^{(p^{g-1})}$ has rank g.*

(iv) *The p-rank of $J(C)$ is g, that is, there are p^g points on $J(C)$ killed by p in $\bar{k}$.*

(v) *$P_\pi(\lambda)$ has g p-adic unit roots in the algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$.*

(vi) *The Newton polygon $\mathfrak{N}(P_\pi)$ has the segments S_1, S_2 with slopes 0 and $-a$, respectively, and looks like Fig. 1.*

(vii) *The p-divisible group $J(p)$ of $J(C)$ is isogenous to $gG_{1,0}$.*

(viii) *The formal group Γ of $J(C)$ has height g and is isogenous to $G_m(p)^g$ where $G_m(p)$ denotes the multiplicative group of height 1 and of dimension 1.*

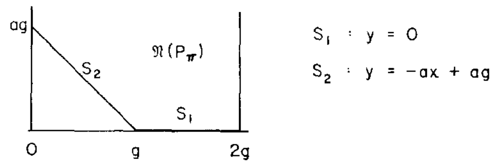


FIGURE 1

DEFINITION 3.1. When $J(C)$ satisfies any one of the conditions in Theorem 3.1, $J(C)$ is called *ordinary*.

Remarks. (1) By the Newton polygon $\mathfrak{N}(P_\pi)$ of $P_\pi(\lambda) = \sum_{i=0}^{2g} a_i\lambda^i \in \mathbb{Z}[\lambda]$, we mean the lower convex envelope of the set of points $\{(i, v_p(a_i)) \mid i = 0,\ldots, 2g\} \subset \mathbb{R} \times \mathbb{R}$ where v_p is the p-adic valuation of $\mathbb{Q}_p$. (2) We denote by ν_p the unique extension of the p-adic valuation v_p to the algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, normalized so that $\nu_p(p) = 1$. (3) The formal group Γ of $J(C)$ is the connected component of the p-divisible group $J(p)$ of $J(C)$.

Proof of Theorem 3.1. (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii) and (v) $\Leftrightarrow$ (vi) are obvious.

(iii) $\Leftrightarrow$ (iv). Since the classes of divisors of order p of K correspond to the points on $J(C)(\bar{k})$ of order p, (iii) $\Rightarrow$ (iv) follows from Corollary 2.3a and (iv) $\Rightarrow$ (iii) from Theorem 2.1 and 2.2.

(i) $\Leftrightarrow$ (v). By the Manin congruence (4), $a_g \equiv (-1)^g \mid A_\pi \mid \pmod{p}$. Now assume (i). Then $v_p(a_g) = 0$. Noting also that $v_p(a_{2g}) = 0$, the Newton polygon $\mathfrak{N}(P_\pi)$ has a segment S_1 of length g and with slope 0. Therefore $P_\pi(\lambda)$ has exactly g p-adic unit roots in $\bar{\mathbb{Q}}_p$, whence the assertion (v). Conversely, assume (v) and let $\tau_1,\ldots, \tau_g$ be the p-adic unit roots of $P_\pi(\lambda)$. As $P_\pi(\lambda)$ has always together with roots τ_i, the roots p^a/τ_i, we have

$$P_\pi(\lambda) = \prod_{i=1}^{g} (\lambda - \tau_i)(\lambda - p^a/\tau_i), \quad \nu_p(\tau_i) = 0 \qquad \text{for all} \quad i = 1,\ldots, g.$$

So $v_p(a_g) = \sum_{i=1}^{g} \nu_p(\tau_i) = 0$. Hence again by the congruence (4), we get $\mid A_\pi \mid \not\equiv 0 \pmod{p}$. This proves (v) $\Rightarrow$ (i).

(vii) $\Leftrightarrow$ (viii). Assume (vii). The p-divisible group $G_{1,0}$ is isogenous to $G_m(p) \times (\mathbb{Q}_p/\mathbb{Z}_p)_k$ where $G_m(p)$ is the multiplicative group of height 1 and $(\mathbb{Q}_p/\mathbb{Z}_p)_k$ is the étale group of height 1. Hence $J(p) \sim gG_{1,0} = G_m(p)^g \times (\mathbb{Q}_p/\mathbb{Z}_p)_k^g$. The assertion (viii) follows from the facts that the connected component of $J(p)$ is the formal group of $J(C)$ and $G_m(p)^g$ is connected of height g. The converse (viii) $\Rightarrow$ (vii) is easy, because if $J(p)$ has the component $G_m(p)^g$, $J(p)$ also has its dual $(\mathbb{Q}_p/\mathbb{Z}_p)_k^g$ as its component.

(v) $\Leftrightarrow$ (vii). First (v) $\Rightarrow$ (vii) is the Manin fundamental theorem 4.1 in [6]. To show the converse, we consider the Dieudonné module $T_p(J) = T_p(G_m(p)^g) \oplus T_p((\mathbb{Q}_p/\mathbb{Z}_p)_k^g)$ corresponding to the p-divisible group $J(p)$. Since $P_\pi(\lambda)$ is the characteristic polynomial of the p-adic representation $T_p(\pi)$ of the Frobenius endomorphism π of $J(C)$ on $T_p(J)$, we may write $P_\pi(\lambda) = P_a(\lambda)\, P_0(\lambda)$ where $P_a(\lambda)$ (resp. $P_0(\lambda)$) is the characteristic polynomial of the restriction of $T_p(\pi)$ to $T_p(G_m(p)^g)$ (resp. to $T_p((\mathbb{Q}_p/\mathbb{Z}_p)_k^g)$). Both $P_a(\lambda)$ and $P_0(\lambda)$ have the same degree g. Moreover, we have

$$P_0(\lambda) = \prod_{i=1}^{g} (\lambda - \tau_i), \quad \nu_p(\tau_i) = 0 \qquad \text{for all} \quad i = 1,\ldots, g.$$

In fact, $(\mathbb{Q}_p/\mathbb{Z}_p)_k^g$ being étale, $T_p(\pi)$ induces an automorphism of $T_p((\mathbb{Q}_p/\mathbb{Z}_p))_k^g)$ and hence all the characteristic roots of $P_0(\lambda)$ must have the p-adic value 0.
Q.E.D.

THEOREM 3.2. *With the notation as in Theorem* 3.1, *suppose that $J(C)$ is elementary and ordinary. Then we have*

(a) *$P_\pi(\lambda)$ is $\mathbb{Q}$-irreducible.*

(b) *The endomorphism algebra $\mathscr{A} = \mathrm{End}_k(J(C)) \otimes Q$ is commutative and coincides with its center $\Phi = \mathbb{Q}(\pi)$.*

(c) *$\Phi = \mathbb{Q}(\pi)$ is a CM-field of degree $2g$. Let $\beta = \pi + \bar{\pi}$ where $\bar{\pi}$ denotes the complex conjugate of π. Then β is totally real and $[\mathbb{Q}(\pi) : \mathbb{Q}] = g$ and $|\beta| < 2p^{a/2}$, $(\beta, p) = 1$, and $P_\pi(\lambda) = \lambda^2 - \beta\lambda + p^a \in \mathbb{Q}(\beta)[\lambda]$.*

(d) *$J(C)$ is k-simple.*

Proof. It is well known that if $J(C)$ is elementary, $P_\pi(\lambda) = P(\lambda)^e$ for some integer e with $P(\lambda)$ $\mathbb{Q}$-irreducible and $P(\pi) = 0$ and that $\mathscr{A}$ is a division algebra of dimension e^2 over its center $\Phi = \mathbb{Q}(\pi)$.

Now suppose that $J(C)$ is elementary and ordinary. Then by Theorem 3.1, $P_\pi(\lambda)$ has the p-adic decomposition

$$P_\pi(\lambda) = \prod_{i=1}^{g} (\lambda - \tau_i)(\lambda - p^a/\tau_i), \qquad \nu_p(\tau_i) = 0 \qquad \text{for every} \quad 1 \leqslant i \leqslant g.$$

Hence at every prime ν over p in Φ, $\operatorname{ord}_\nu(\pi) = 0$ or a. Thus the local invariant i_ν of $\mathscr{A}$ at ν (defined by Tate [13] as $i_\nu = \operatorname{ord}_\nu(\pi) \cdot f_\nu/a$ where f_ν is the residue degree at ν) is an integer for every ν over p. Noting that there are no real primes, (because if π is real, $\pi = \pm p^{a/2}$ and $\operatorname{ord}_\nu(\pi) = a/2$), we see that the least common denominator of all the i_ν is 1. Since e is the period of $\mathscr{A}$ in the Brauer group of Φ and so is the least common denominator of all the i_ν, we get $e = 1$, whence the assertions (a), (b), and (d).

Now we shall prove (c). Since π is imaginary with $\deg(\pi) = 2g$, $\mathbb{Q}(\pi)$ is a CM-field of degree $2g$. Put $\beta = \pi + \bar{\pi}$. In every embedding $\Phi = \mathbb{Q}(\pi)$ into $\mathbb{C}$, $|\pi| = p^{a/2}$ by the Riemann hypothesis, so $\beta = \pi + p^a/\pi$ is real and $\mathbb{Q}(\beta)$ becomes totally real with $[\mathbb{Q}(\beta) : \mathbb{Q}] = g$ and $\mathbb{Q}(\pi)$ becomes imaginary over it (i.e., π satisfies the equation $P_\pi(\pi) = \pi^2 - \beta\pi + p^a = 0$ over $\mathbb{Q}(\beta)$). As $J(C)$ is ordinary by the hypothesis, $P_\pi(\lambda)$ must split. Hence at every prime ν over p, we have $\operatorname{ord}_\nu(\beta) = 0$, whence $(\beta, p) = 1$. Q.E.D.

EXAMPLE 3.3. Consider the curve $C: y^2 = 1 - x^5$ defined over the prime field $\mathbb{F}_p$ where p is a prime of the form $10n + 1$, $n \in \mathbb{N}$. C has genus 2 and the Cartier–Manin matrix A of C is given by

$$A = \begin{pmatrix} \binom{(p-1)/2}{(p-1)/5} & 0 \\ 0 & \binom{(p-1)/2}{2(p-1)/5} \end{pmatrix} \quad \text{with } (:) \text{ binomial coefficient.}$$

It is easy to see that $|A| \neq 0$ in $\mathbb{F}_p$. So $J(C)$ is ordinary by Theorem 3.1. We have

$$P_\pi(\lambda) \equiv \lambda^4 - \left\{ \binom{(p-1)/2}{(p-1)/5} + \binom{(p-1)/2}{2(p-1)/5} \right\} \lambda^3 + |A| \lambda^2 \pmod{p}.$$

So $P_\pi(\lambda)$ must split with roots of orders 0 and 1. Hence half the places have $\operatorname{ord}_\nu(\pi) = 0$ and the other half have $\operatorname{ord}_\nu(\pi) = 1$. So i_ν is an integer for every prime ν over p, and hence $J(C)$ is simple over $\mathbb{F}_p$.

This is a rather special example (cf. Honda [3]). Let ζ be the endomorphism of $J(C)$ corresponding to the birational automorphism $(x, y) \to (\zeta x, y)$ of C. Put $L = \mathbb{Q}(\zeta)$. Then L is the decomposition field of $p = 10n + 1$ with $[L : \mathbb{Q}] = 4$ and moreover $L = \mathbb{Q}(\pi)$. Since $\mathscr{A}$ contains a field L of degree 4, $J(C)$ is isogenous to a product of a simple abelian variety. But p splits in Φ and the local invariants of $\mathscr{A}$ are all integers. Hence $\mathscr{A} = \Phi = L = \mathbb{Q}(\zeta)$. This shows that for all primes p of the form $10n + 1$, $n \in \mathbb{N}$, $J(C)$ are of the same CM-type (L) and hence are isogenous to each other.

4. The Jacobian Variety $J(C)$ of C with $|A| = 0$

Theorem 4.1. *With the notation as in Section* 3, *suppose that the Cartier–Manin matrix A of C has the determinant $|A| = 0$ in k. Then we have* (a) *If the matrix $A\,A^{(p)} \cdots A^{(p^{a-1})}$ has rank 0, then the matrix $A\,A^{(p)} \cdots A^{(p^{g-1})}$ also has rank 0.*

(b) *When* (a) *is the case, the following statements are equivalent*:

(bi) *The p-rank of $J(C)$ is 0, that is, there are no points on $J(C)$ defined over $\bar{k}$, killed by p.*

(bii) *The characteristic polynomial $P_\pi(\lambda)$ has the p-adic decomposition $P_\pi(\lambda) = \prod_{i=1}^{2g} (\lambda - \tau_i)$ with $0 < \nu_p(\tau_i) < a$.*

(biii) *The formal group Γ of $J(C)$ has height $2g$ and coincides with the p-divisible group $J(p)$ of $J(C)$.*

Proof. (a) Let $l \geqslant 1$ be an integer and let us denote by ρ_l the rank of the matrix $A_l = A\,A^{(p)} \cdots A^{(p^{l-1})}$, and $A_0 = I_g$.

Suppose now that $A_\pi = A\,A^{(p)} \cdots A^{(p^{a-1})}$ has rank 0. If $a \leqslant g$, there is nothing to prove. So we assume now that $a > g$. Let R_l be the k-vector space of the roots of the system of equations $\mathscr{C}^l\mathbf{x} = \mathbf{0}$ in $\bar{k}$, i.e., $R_l = \{\mathbf{x} \mid \mathscr{C}^l\mathbf{x} = A_l\mathbf{x}^{p^l} = \mathbf{0}\}$, $R_0 = \{0\}$ and $R_g = H$ (in Theorem 2.1). We know that the rank of R_l is $g - \rho_l$. First we shall prove the following lemma.

Lemma. *Put $\delta_l = \rho_{l-1} - \rho_l$. Then δ_l is the rank of the k-vector space R_l/R_{l-1} and*

$$\delta_1 \geqslant \delta_2 \geqslant \cdots \geqslant \delta_g \geqslant \delta_{g+1} = \cdots = \delta_n = 0 \qquad \textit{for any} \quad n \geqslant g + 1.$$

Proof of Lemma. It is easily seen that $R_l \supset R_{l-1}$ and $\delta_l = (g - \rho_l) - (g - \rho_{l-1})$ is the rank of the space R_l/R_{l-1}. Let $\mathbf{u}_1^{(g)},\ldots, \mathbf{u}_{\delta_g}^{(g)}$ be a basis of R_g/R_{g-1}. Applying the Cartier operator $\mathscr{C}$, we get

$$\mathscr{C}\mathbf{u}_1^{(g)},\ldots, \mathscr{C}\mathbf{u}_{\delta_g}^{(g)} \in R_{g-1},$$

and modulo R_{g-2}, they are linearly independent. Hence we get the inequality $\delta_g + g - \rho_{g-2} \leqslant g - \rho_{g-1}$, whence $\delta_{g-1} \geqslant \delta_g$. Continuing the same discussion, we have $\delta_1 \geqslant \delta_2 \geqslant \cdots \geqslant \delta_g$. It remains to show that $\delta_g \geqslant \delta_{g+1} = \cdots = \delta_n = 0$. But this is an immediate consequence of Theorem 2.1, because $R_g = R_n$ for every $n \geqslant g + 1$. Q.E.D.

Now we shall prove the theorem. The assertion (a) follows immediately from the lemma. In fact, take $n = a$, then $\rho_a = 0$ by the hypothesis and $\rho_g = \rho_{g+1} = \cdots = \rho_a = 0$.

(b) We shall prove (a) $\Rightarrow$ (bi) $\Rightarrow$ (bii) $\Rightarrow$ (biii) $\Rightarrow$ (bi).

(a) $\Rightarrow$ (bi). See Corollary 2.3 b.

(bi) $\Rightarrow$ (bii). We first note that the p-rank of $J(C)$ coincides with the rank of the toroidal component $G_{1,0}$ of $J(p)$. As we have seen in the proof of Theorem 3.1(v) $\Leftrightarrow$ (vii), the characteristic roots of $P_\pi(\lambda)$ corresponding to the toroidal component have the p-adic values 0 and a. Now assume (bi). Then (bii) follows from the above fact and from the Riemann hypothesis that all the characteristic roots must have the absolute value $p^{a/2}$.

(bii) $\Rightarrow$ (biii). Assume (bii). Then by the Manin theorem 4.1 in [6], the p-divisible group $J(p)$ of $J(C)$ has no toroidal component. So $J(p)$ is connected. Hence the formal group Γ of $J(C)$ has height $2g$ and coincides with the p-divisible group $J(p)$.

(biii) $\Rightarrow$ (bi). This is a trivial consequence of the fact that the p-rank of $J(C)$ is equal to the rank of the toroidal component of $J(p)$. Q.E.D.

Remarks 4.2. (1) The Cartier–Manin matrix A of C in Theorem 4.1 provides us merely a connected p-divisible group of height $2g$. So in order to determine the local structure of $J(C)$ up to isogeny, we must classify the connected p-divisible groups of height $2g$ into isogeny classes. Manin [6] is the first to observe that the local decomposition of $J(C)$ parallels the p-adic factorization of the characteristic polynomial $P_\pi(\lambda)$ of π.

(2) Let $2s$ (resp. r) be the number of the p-adic roots τ_i of $P_\pi(\lambda)$ with $\nu_p(\tau_i) = a/2$ (resp. 0). Then we can factor $P_\pi(\lambda)$ into the form

$$P_\pi(\lambda)$$

$$= \prod_{\substack{i=1\\ \nu_p(\tau_i)=a/2}}^{2s} (\lambda - \tau_i) \cdot \prod_{\substack{i=1\\ \nu_p(\tau_i)=0}}^{r} (\lambda - \tau_i)(\lambda - p^a/\tau_i) \cdot \prod_{\substack{i=1\\ 0<\nu_p(\tau_i)<a/2}}^{g-s-r} (\lambda - \tau_i)(\lambda - p^a/\tau_i).$$

(Note that $J(p)$ is connected, if and only if $r = 0$.)

In the forthcoming sections, we shall determine, up to isogeny, the type of the formal group Γ, of the p-divisible group $J(p)$ and then the algebraic structure of $J(C)$ up to isogeny, in the cases, $[s = g, r = 0]$, $[s = 0, r = 0]$, and $[0 < s < g, 0 < r < g]$, respectively.

(3) In principle, the characteristic polynomial $P_\pi(\lambda)$ can be explicitly determined by making use of the well-known Lefsechtz formulas for the hyperelliptic curve C over k (cf. [5]).

5. Supersingular Jacobian Variety $J(C)$ of C

Theorem 5.1. *Suppose that the Cartier–Manin matrix A of C has the determinant $|A| = 0$ in k and that the matrix A_π has rank 0. Then we have*

(a) *The following statements are equivalent:*

(ai) *$s = g$, i.e, all the characteristic roots of $P_\pi(\lambda)$ have the p-adic value $a/2$.*

(aii) *The Newton polygon $\mathfrak{N}(P_\pi)$ has only one nonvertical segment with slope $-a/2$ and looks like Fig. 2.*

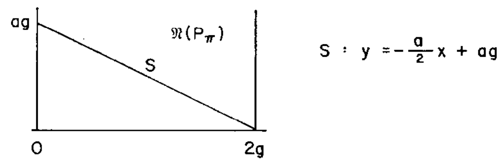


Figure 2

(b) *When* (a) *is the case, the p-divisible group $J(p)$ of $J(C)$ is isogenous to $gG_{1,1}$ and so is the formal group Γ of $J(C)$.*

(c) *The following statements are equivalent:*

(ci) *The p-divisible group $J(p)$ of $J(C)$ has the isogeny type $gG_{1,1}$.*

(cii) *The Newton polygon of the characteristic polynomial of π^n for some integer $n \geqslant 1$ has only one nonvertical segment with slope $-an/2$.*

Definition 5.1. When $J(C)$ has the p-divisible group $J(p)$ isogenous to $gG_{1,1}$, $J(C)$ is called *supersingular*.

Proof of Theorem 5.1. (a) (ai) $\Rightarrow$ (aii). By the hypothesis,

$$P_\pi(\lambda) = \prod_{\substack{i=1 \\ v_p(\tau_i)=a/2}}^{2g} (\lambda - \tau_i) = \sum_{i=0}^{2g} a_i\lambda^i.$$

So we have $v_p(a_i) = (2g - i)\, a/2$ for every $0 \leqslant i \leqslant 2g$. Hence the equation for the nonvertical segment of $\mathfrak{N}(P_\pi)$ is given by $y = -(a/2)x + ag$.

(aii) $\Rightarrow$ (ai). Clear.

(b) This follows from the Manin theorem 4.1 in [6], and Theorem 4.1b.

(c) First note that over any finite extension k_n of k of degree $n \geqslant 1$, there exists an Abelian variety B_n of dimension g whose all the characteristic roots of the Frobenius endomorphism relative to k_n have the p-adic value $an/2$. (For example, $B_n = E^g$ where E is an elliptic curve with vanishing Hasse invariant.) Then by Manin's Theorem 4.1 in [6], B_n has the p-divisible group

$B_n(p)$ isogenous to $gG_{1,1}$. There is a one-to-one correspondence due to Tate (see Waterhouse [15]) and to Manin:

$$\mathrm{Hom}_{k_n}(J(C), B_n) \otimes \mathbb{Z}_p \leftrightarrow \mathrm{Hom}_{k_n}(J(p), B_n(p)).$$

(ci) $\Rightarrow$ (cii) Now suppose (ci). Then there exists an element $\phi(p) \in \mathrm{Hom}_{k_n}(J(p), B_n(p)) \subseteq \mathrm{Hom}_{\bar{k}}(gG_{1,1}, gG_{1,1}) = \mathrm{End}_{\bar{k}}(gG_{1,1}) \simeq M_g(\mathrm{End}_{\bar{k}}(G_{1,1}))$ (M_g denotes the $(g \times g)$ matrix algebra.) By the above correspondence, we get the element $\phi \in \mathrm{Hom}_{k_n}(J(C), B_n)$. Hence the characteristic polynomial of $\pi^n_{J(C)} = \pi^n$ coincides with that of the Frobenius endomorphism π_{B_n} of B_n relative to k_n. Therefore the p-adic exponents of the eigenvalues of π^n are $an/2$. Thus (cii) follows from by applying the argument (ai) $\Rightarrow$ (aii) with π^n for π.

(cii) $\Rightarrow$ (ci). Suppose (cii). Then there are $2g$ characteristic roots with p-adic value $an/2$. Hence by applying the Manin Theorem 4.1 in [6] with k_n for k and π^n for π, the p-divisible group $J(p)$ of $J(C)$ is isogenous to $gG_{1,1}$.

Q.E.D.

THEOREM 5.2. *A supersingular Jacobian variety $J(C)$ of C over k is isogenous over some finite extension of k to a product $E \times \cdots \times E$ (g copies) of a supersingular elliptic curve E (cf. Oort* [9]).

Proof. Recall that an elliptic curve is called supersingular if its endomorphism algebra is noncommutative. We employ the same notation as in Theorem 3.2: $\mathscr{A}$ the endomorphism algebra of $J(C)$ and $\Phi = \mathbb{Q}(\pi)$ the center of $\mathscr{A}$. The algebraic integer π satisfying the Riemann hypothesis $|\pi| = p^{a/2}$ in all embedding of Φ into $\mathbb{C}$, are called the Weil numbers. As the notation suggests, we may identify the Frobenius endomorphism with a Weil number.

Now by the assumption, all the characteristic roots of $P_\pi(\lambda)$ have the p-adic value $a/2$.

I. Suppose that there are real primes in Φ.

Case Ia. If a is even, $\pi = \pm p^{a/2}$ is rational. Hence $\Phi = \mathbb{Q}$, $P_\pi(\lambda) = (\lambda \pm p^{a/2})^{2g}$, $[\mathscr{A} : \mathbb{Q}] = (2g)^2$, and $\mathscr{A} = M_g(Q_{p,\infty}) : a$ $(g \times g)$ matrix algebra over the quaternion algebra $Q_{p,\infty}$ over $\mathbb{Q}$ which is ramified only at p and ∞. Then by Tate [13], $J(C)$ is isogenous over k to g copies of a supersingular elliptic curve over k, all of whose endomorphisms are defined over k and whose characteristic polynomial is $(\lambda \pm p^{a/2})^2$.

Case Ib. If a is odd, $\pi = \pm p^{a/2} \notin \mathbb{Q}$, but π^2 becomes rational. We have $\Phi = \mathbb{Q}(p^{1/2})$, $[\Phi : \mathbb{Q}] = 2$. So there are two infinite primes with local invariants $\frac{1}{2}$, and only one prime over p with local invariant 0. Thus the least common denominator of all the local invariants is 2. Hence we obtain a k-simple constituent X of $J(C)$ with $\dim X = \frac{1}{2} \cdot 2 \cdot \deg(\pi) = 2$. Passing to the quadratic extension k_2 of k, we have $\mathbb{Q}(\pi^2) = \mathbb{Q}$ and X becomes isogenous to the product of a supersingular elliptic curve. Hence by applying the same argument as in Case Ia, the algebra $\mathscr{A}^{(2)}$ attached to $J(C)$ relative to k_2 becomes a matrix algebra over $Q_{p,\infty}$ and the characteristic polynomial of π^2 is given by $P_{\pi^2}(\lambda) = (\lambda - p^a)^{2g}$. Hence $J(C)$ is isogenous over k_2 to g copies of a supersingular elliptic curve over k_2.

II. Suppose now that there are no real primes in Φ. So $\mathbb{Q}(\pi)$ is totally imaginary. Put $\beta = \pi + p^a/\pi$. Then β is real and $\mathbb{Q}(\beta)$ becomes totally real and $\mathbb{Q}(\pi)$ is imaginary quadratic over it. We can write $P_\pi(\lambda) = \lambda^2 - \beta\lambda + p^a \in \mathbb{Q}(\beta)[\lambda]$ with $|\beta| < 2p^{a/2}$. The solution of $P_\pi(\lambda) = 0$ is a Weil number. Now the hypothesis that all the characteristic roots of $P_\pi(\lambda) = 0$ have the p-adic value $a/2$ implies that $(\beta, p) \neq 1$ and hence p ramifies or stays prime in $\mathbb{Q}(\beta)$. Write $\beta = \pm p^b\alpha$ with $b \in \mathbb{Q}$ and $\alpha = 0$ or an algebraic integer satisfying $(\mathrm{Norm}(\alpha), p) = 1$.

Case IIa. If $\alpha = 0$, then $\beta = 0$ and $\mathbb{Q}(\beta) = \mathbb{Q}$, $\mathbb{Q}(\pi) = \mathbb{Q}((-p^a)^{1/2})$ with $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2$. Hence we get Weil numbers $\pi = \pm p^{a/2} \cdot \sqrt{-1}$, whose second powers become rational. So if a is odd or a is even and $p \not\equiv 1 \pmod 4$, they give supersingular elliptic curves whose all endomorphisms are not defined over k, but are defined over k_2. Hence the characteristic polynomial of π^2 is given by $P_{\pi^2}(\lambda) = (\lambda + p^a)^{2g}$, and hence $J(C)$ is isogenous over k_2 to g copies of a supersingular elliptic curve over k_2.

Case IIb. If $\alpha \neq 0$ and $2b < a$, then we have $\pi = \pm(p^b\alpha \pm p^b(\alpha^2 - 4p^{a-2b})^{1/2})/2$. Since $\alpha^2 - 4p^{a-2b} \equiv \alpha^2 \pmod{4p}$, we have $\nu_p(\pi) = b < a/2$. But this contradicts to our hypothesis. So we can suppose that $2b \geqslant a$. As $\beta^2 - 4p^a = p^a(p^{2b-a}\alpha^2 - 4) < 0$ and $p \neq 2$, we must have $|p^{b-a/2}| < 2$. So it follows that $\pi = \pm p^{a/2}(p^{b-a/2}\ \alpha \pm i\,|p^{2b-a}\alpha^2 - 4|^{1/2})/2$ with $\mathrm{Norm}((p^{b-a/2}\alpha \pm i\,|p^{2b-a}\alpha^2 - 4|^{1/2})/2) = 1$. Hence $\nu_p(\pi) = a/2$. Since $|p^{b-a/2}\alpha| < 2$, we have $|p^{b-a/2}\alpha/2| < 1$ and $|p^{2b-a}\alpha^2 - 4|^{1/2}/2 < 1$. Hence $(p^{b-a/2}\alpha \pm i|p^{2b-a}\alpha^2 - 4|^{1/2})/2$ is a root of unity. Therefore some powers of π becomes rational, say $\pi^t = \pm p^{ta/2} \in \mathbb{Q}$. So if a is even (resp. odd), the characteristic polynomial of π^t (resp. π^{2t}) is given by $P_{\pi^t}(\lambda) = (\lambda \pm p^{ta/2})^{2g}$ (resp. $P_{\pi^{2t}}(\lambda) = (\lambda \pm p^{at})^{2g}$), whence $J(C)$ is isogenous over the extension k_t of degree t (resp. k_{2t} of degree $2t$) of k to g copies of a supersingular elliptic curve over k_t (resp. k_{2t}).

A typical example of Case IIb is when the characteristic polynomial $P_\pi(\lambda)$ of π of $J(C)$ relative to k is given by $P_\pi(\lambda) = \lambda^{2g} + p^{ag}$. Q.E.D.

It is a classical result that an elliptic curve E over k is supersingular if and only if the Hasse invariant of E is zero. In the following, we shall give a generalization of this fact to higher-dimensional cases.

THEOREM 5.3. *Suppose that the Cartier–Manin matrix A of C is* (0) *in k. Then $J(C)$ is supersingular and is isogenous over some finite extension of k to g copies of a supersingular elliptic curve.*

Proof. $A = (0)$ certainly satisfies the hypothesis of Theorem 4.1(a), so that $J(p)$ has no toroidal components $\Leftrightarrow$ $J(C)$ has no p-torsion points $\Leftrightarrow$ The Tate group of the dual of $J(C)$ is 0. First we shall prove the following two lemmas.

LEMMA A. *Let F be the Frobenius morphism of $K = k(x, y)$ onto $K^p = k^p(x^p, y^p)$, $J(C)$ onto $J(C)^{(p)}$ and $J(p)$ onto $J(p)^{(p)}$ induced by the pth power map $a \to a^p$ of k and $F' = V$ its dual morphism. Then for the canonical basis $\boldsymbol{\omega} = (\omega_1, \dots, \omega_g)$ of $\mathfrak{D}_0(K)$ $(\simeq \mathfrak{D}_0(J(C)))$ given as* (3), *we have*

$$\mathscr{C}'\boldsymbol{\omega} = \boldsymbol{\omega} \circ V = A^{(1/p)}\boldsymbol{\omega}, \qquad \mathscr{C}\boldsymbol{\omega} = \boldsymbol{\omega} \circ F = A\boldsymbol{\omega}^p.$$

Proof of Lemma A. Let $\mathfrak{O}$ be the ring of integers in the absolutely unramified extension L of $\mathbb{Q}_p$ with residue field $k = \mathbb{F}_{p^a}$. So p generates the maximal ideal of $\mathfrak{O}$. We can lift the equation for C to L, which we write $\tilde{C} : y^2 = \tilde{f}(x)$ where $\tilde{f}$ is a polynomial over $\mathfrak{O}$ without multiple roots of degree $2g + 1$ such that $\tilde{C} \bmod p = C$. Let $t_i = x^i/y$, $i = 1, \dots, g$ and $\mathbf{t} = (t_1, \dots, t_g)$. As we have seen in Section 2, $\mathbf{t}$ is a system of local parameters of C at the origin and the canonical basis ω_i, $i = 1, \dots, g$ of $\mathfrak{D}_0(K)$ can be written as

$$\omega_i = d\phi_i + \sum_{l=1}^{g} c_{lp-i} t_l{}^p \frac{dx}{x}, \qquad \phi_i \in K.$$

Now the differential forms of degree 1 and of the first kind on the algebraic function field of $\tilde{C}$ can have the form

$$\tilde{\omega}_i = d\tilde{\phi}_i + \sum_{l=1}^{g} \tilde{c}_{lp-i} t_l{}^p \frac{dx}{x} \qquad \text{with} \quad \tilde{\omega}_i \bmod p = \omega_i \quad \text{for} \quad i = 1, \dots, g.$$

Let $\tilde{\mathbf{\Gamma}} = (\tilde{\Gamma}_i)$, $i = 1, \dots, g$ be the formal group of $J(\tilde{C})$ with respect to the local parameters $\mathbf{t}$, so that $\tilde{\mathbf{\Gamma}} \bmod p = \mathbf{\Gamma}$. We consider the isogeny of $\mathbf{\Gamma}$ (resp. $\tilde{\mathbf{\Gamma}}$) of multiplication by p. On $\tilde{\mathbf{\Gamma}} = (\tilde{\Gamma}_i)$ over $\mathfrak{O}$, there exist systems of power series $\tilde{\mathbf{U}}(\mathbf{t}) = (\tilde{U}_i(\mathbf{t}))$, $\tilde{\mathbf{W}}(\mathbf{t}) = (W_i(\mathbf{t}))$ in $\mathfrak{O}[[\mathbf{t}]]$ such that

$$\tilde{\mathbf{W}}(\mathbf{t}) = \mathbf{1} + \cdots,$$
$$\mathbf{t} \circ (p1_{\tilde{\Gamma}}) = p\tilde{\mathbf{W}}(\mathbf{t}) + \tilde{\mathbf{U}}(\mathbf{t}^p).$$

So by reducing modulo p, we get

$$\mathbf{t} \circ (p1_{\Gamma}) = \mathbf{U}(\mathbf{t}^p) = (U_i(\mathbf{t}^p)), \qquad \text{where} \quad \mathbf{U} = \tilde{\mathbf{U}} \bmod p.$$

Now we know that in characteristic $p > 0$, the multiplication by p can be expressed as the product of F and V taken in either order: $p1_{\Gamma} = FV = VF$ (cf. Manin [6, Proposition 1.4]). So we have

$$\mathbf{t} \circ F = \mathbf{t}^p, \qquad \mathbf{t} \circ V = \mathbf{t} \circ (p1_{\Gamma}/F) = (\mathbf{b}_1\mathbf{t}, \dots, \mathbf{b}_g\mathbf{t}),$$

where $\mathbf{b}_i\mathbf{t} = \sum_{l=1}^{g} b_{li}t_l$ with b_{li} the coefficient of $t_l{}^p$ in $U_i(\mathbf{t}^p)$. Expanding $\tilde{\omega}_i$ into power series of $\mathbf{t} = (t_1,\ldots,t_g)$, we have

$$\tilde{\omega}_i = \sum_{l=1}^{g} dt_l(\tilde{a}_{li} + \cdots + \tilde{c}_{lp-i}t_l^{p-1} + \cdots) = \sum_{l=1}^{g} \tilde{h}_{li}(t_l)\, dt_l\,,$$

where $\tilde{a}_{li} \equiv 1 \pmod p$ for all i, l. So it follows that

$$\tilde{\omega}_i \circ (p1_{\tilde{\Gamma}}) = p\tilde{\omega}_i = \sum_{l=1}^{g} p\tilde{h}_{li}(t_l)\, dt_l\,.$$

On the other hand, we also have

$$\tilde{\omega}_i \circ (p1_{\tilde{\Gamma}}) = \sum_{l=1}^{g} \tilde{h}_{li}(\tilde{U}_i(t_l{}^p) + p\tilde{W}_i(t_l)) \cdot (\tilde{U}_i'(t_l{}^p)\, pt_l^{p-1} + p\tilde{W}_i'(t_l))\, dt_l\,.$$

Hence we get the equality

$$\sum_{l=1}^{g} \tilde{h}_{li}(t_l)\, dt_l = \sum_{l=1}^{g} \tilde{h}_{li}(\tilde{U}_i(t_l{}^p) + p\tilde{W}_i(t_l)) \cdot (\tilde{U}_i'(t_l{}^p)\, t_l^{p-1} + \tilde{W}_i(t_l))\, dt_l\,.$$

Read it modulo p and compare the coefficients of t_l^{p-1} of both sides for each $l = 1,\ldots, g$. Since

$$\tilde{h}_{li}(\tilde{U}_i(t_l{}^p) + p\tilde{W}_i(t_l)) \equiv \tilde{h}_{li}(\tilde{U}_i(t_l{}^p)) \equiv 1 \qquad \pmod p,$$

and

$$U_i'(t_l{}^p) = b_{li}\,,$$

we get $c_{lp-i} = b_{li}$ for i, $l = 1,\ldots, g$. This proves that

$$\mathscr{C}'\omega_i = \sum_{l=1}^{g} c_{lp-i}^{1/p}\omega_l = \omega_i \circ V.$$

By duality, we also get

$$\mathscr{C}\omega_i = \sum_{l=1}^{g} c_{lp-i}\omega_l{}^p = \omega_i \circ F. \qquad \text{Q.E.D.}$$

LEMMA B. *The hypothesis and the notation are as in Theorem* 5.3 *and Lemma* A. *Then* $p1_{J(C)} = p1_\Gamma$, F *and* V *are purely inseparable and moreover, we have*

$$F^2 = V^2 = -p1_{J(C)}\,.$$

Proof of Lemma B. Since $J(C)$ has no points of order p in $\bar{k}$, $p1_{J(C)}$ is purely inseparable of degree p^{2g} (cf. [12, Chap. I, Proposition 7]). According to Serre [11], every purely inseparable isogeny is the product of elementary isogenies of height 1, of one of two types i_1, i_2 defined as follows. Let $\mathfrak{N}$ be the p-Lie algebra of differentiations of $J(C)$. The isogeny of type i_1 corresponds to the subspace $\{\partial \in \mathfrak{N} \mid \partial^p = 0\}$ of $\mathfrak{N}$ and that of type i_2 to the subspace $\{\partial \in \mathfrak{N} \mid \partial^p = \partial\}$ of $\mathfrak{N}$. The dual (or the transpose) of type i_1 is again of type i_1 and has kernel 0, while that of type i_2 becomes separable and has kernel of order p. Since the Cartier–Manin matrix A of C is the matrix of the map $\partial \to \partial^p$ in $\mathfrak{N}$, $A = (0)$ implies that V is the g product of the isogenies of type i_1. So it is purely inseparable of degree p^g. It follows that F is also the g product of the dual of the isogenies of type i_1. Hence F is also purely inseparable of degree p^g. Therefore, F^2, V^2, and $p1_{J(C)}$ are purely inseparable of degree p^{2g} and they differ only by an automorphism. Let σ be an automorphism of K (modulo translation automorphism). σ has the form: $x^\sigma = \epsilon x$, $y^\sigma = \eta y$ where ϵ, η roots of unity (cf. [10]). It has the matrix representation $M(\sigma)$ of degree g with respect to the canonical basis ω_i, $i = 1,\dots, g$ of $\mathfrak{D}_0(K)$:

$$(\omega_i^\sigma,\dots, \omega_g^\sigma) = M(\sigma)(\omega_1,\dots, \omega_g).$$

$M(\sigma)$ can be put into the form

$$\begin{pmatrix} \epsilon_1 & & 0 \\ & \ddots & \\ 0 & & \epsilon_g \end{pmatrix},$$

where ϵ_i roots of unity. In particular, the hyperelliptic automorphism is represented by the matrix

$$\begin{pmatrix} -1 & & 0 \\ & \ddots & \\ 0 & & -1 \end{pmatrix}.$$

Now if $A = (0)$, then ω_i, $i = 1,\dots, g$ are given by

$$\omega_i = d\left(y^{-p} \sum_{j+i \not\equiv 0 \pmod p} c_j \frac{x^{j+i}}{j+i}\right), \qquad 0 \leqslant j \leqslant \frac{p-1}{2}(2g+1).$$

Under the automorphism σ, ω_i is transformed to

$$\omega_i^\sigma = d\left(y^{-p}\eta^{-p} \sum_{j+i \not\equiv 0 \pmod p} \epsilon^{j+i} c_j \frac{x^{j+i}}{j+i}\right).$$

But the identity $\omega_i^\sigma = \epsilon_i \omega_i$ for $i = 1,\dots, g$ must hold. Thus the only possibility is when $\eta = \pm 1$ and $\epsilon = 1$, whence $\epsilon_i = \pm 1$ for every i. Thus all the nontrivial automorphisms have order 2. Hence we have $F^2 = -p1_{J(C)}$ and $V^2 = p^2/F^2 = -p1_{J(C)}$. Q.E.D.

The end of the proof of Theorem 5.3. $\pi = F^a$, $\pi' = p^a/F^a$ are purely inseparable isogenies of $J(C)$. The characteristic polynomial of π^2 is given by $P_{\pi^2}(\lambda) = (\lambda + p^a)^{2g}$. Hence $\nu_p(\pi) = a/2$ and $J(p) \sim gG_{1,1}$. Thus $J(C)$ is supersingular by Theorem 5.1. Q.E.D.

EXAMPLE 5.4. $A = (0)$ is a sufficient condition for $J(C)$ to be supersingular, but it is not a necessary one. We shall illustrate some examples that $J(C)$ with $A \neq (0)$ becomes supersingular.

Let C be the hyperelliptic curve of genus 3 with the equation $y^2 = 1 - x^7$ defined over the prime field $\mathbb{F}_p$ of characteristic $p > 2$. The Cartier–Manin matrix A of C is given by $A = (c_{m,n})_{m,n=1,2,3}$, where

$$c_{m,n} = \binom{(p-1)/2}{(mp-n)/7} \cdot (-1)^{(mp-n)/7} \qquad \text{with} \quad c_{m,n} = 0 \quad \text{if} \quad 7 \nmid mp - n.$$

Let ζ be a primitive seventh root of unity and put $L = \mathbb{Q}(\zeta)$. So $[L : \mathbb{Q}] = 6$. Now for any prime $p \neq 7$, there exists the smallest positive integer f such that $p^f \equiv 1 \pmod 7$ and $fr' = 6$ where r' is the degree (over $\mathbb{Q}$) of the decomposition field K_0 of p.

Case I. If $p \equiv 3$ or $5 \pmod 7$, then $p^6 \equiv 1 \pmod 7$, so $f = 6$, $r' = 1$. Hence p stays prime in L. For primes $p \equiv 3 \pmod 7$, the Cartier–Manin matrix A of C has the form

$$c_{1,3} = \binom{(p-1)/2}{(p-3)/7} \cdot (-1)^{(p-3)/7},$$

$$c_{3,2} = \binom{(p-1)/2}{(3p-2)/7} \cdot (-1)^{(3p-2)/7}, \qquad \text{and} \qquad c_{m,n} = 0, \text{ otherwise.}$$

For primes $p \equiv 5 \pmod 7$, the Cartier–Manin matrix A of C has the form

$$c_{2,3} = \binom{(p-1)/2}{(2p-3)/7} \cdot (-1)^{(2p-3)/7},$$

$$c_{3,1} = \binom{(p-1)/2}{(3p-1)/7} \cdot (-1)^{(3p-1)/7}, \qquad \text{and} \qquad c_{m,n} = 0, \text{ otherwise.}$$

In both cases, $|A| = 0$ and $A \neq (0)$, $A\,A^{(p)} \neq (0)$, but $A\,A^{(p)}A^{(p^2)} = (0)$.

Case II. If $p \equiv 6 \pmod 7$, we have $p^2 \equiv 1 \pmod 7$, so $f = 2$, $r' = 3$. Hence p decomposes in the real cubic field $K_0 = Q(\zeta + \zeta^{-1})$. In this case, the Cartier–Manin matrix A of C is $A = (0)$.

Now let π be the pth power endomorphism of $J(C)$ relative to $\mathbb{F}_p$. Then $\pi^f \in K_0$ and the characteristic polynomial of π^f is given as follows:

$$\begin{aligned} P_{\pi^f}(\lambda) &= (\lambda + p^3)^6 \qquad \text{if} \quad \text{Case I}, \\ &= (\lambda + p)^6 \qquad \text{if} \quad \text{Case II}. \end{aligned}$$

(Cf. Honda [3].) Hence $J(p)$ is isogenous to $3G_{1,1}$ in both cases. In Case I (resp. Case II), $J(C)$ is isogenous over the extension of $\mathbb{F}_p$ of degree 6 (resp. over the quadratic extension of $\mathbb{F}_p$) to 3 copies of a supersingular elliptic curve.

6. The Jacobian Variety $J(C)$ of C with the Symmetric Formal Group

Theorem 6.1. *Suppose that the Cartier–Manin matrix A of C has the determinant $|A| = 0$ in k and that the matrix $A_\pi = A\, A^{(p)} \cdots A^{(p^{a-1})}$ has rank 0. Then we have*

(a) *The following statements are equivalent:*

(ai) $s = 0$ *and* $P_\pi(\lambda) = \prod_{i=1}^{g} (\lambda - \tau_i)(\lambda - p^a/\tau_i)$ *with* τ_i *simple roots, and* $v_p(\tau_i) = ac$, $0 < c < \frac{1}{2}$ *for every* $1 \leqslant i \leqslant g$.

(aii) $P_\pi(\lambda) = \sum_{i=0}^{2g} a_i \lambda^i$ *is a distinguished polynomial over* $\mathbb{Z}_p$ *and the coefficients* a_i *satisfy the conditions:*

$$\operatorname*{Min}_{0 \leqslant i \leqslant 2g} \frac{v_p(a_i)}{a(2g - i)} = \frac{v_p(a_g)}{ag} = c = \frac{n_c}{n_c + m_c},$$

where n_c, m_c *are positive integers such that* $1 \leqslant n_c < m_c$, $(n_c, m_c) = 1$, *and* $n_c + m_c = g$.

(aiii) *The p-divisible group* $J(p)$ *of* $J(C)$ *is isogenous to* $G_{n_c, m_c} + G_{m_c, n_c}$ *where* n_c, m_c *are integers such that* $1 \leqslant n_c < m_c$, $(n_c, m_c) = 1$, *and* $n_c + m_c = g$ *and so is the formal group* Γ *of* $J(C)$.

(b) *When* (a) *is the case, the Newton polygon* $\mathfrak{N}(P_\pi)$ *of* $P_\pi(\lambda)$ *has two segments* S_1, S_2 *indexed from the right with slopes* $-ac$, $-a(1 - c)$, *respectively. The vertices of* $\mathfrak{N}(P_\pi)$ *are* $(2g, 0)$, $(g, v_p(a_g))$, *and* $(0, ag)$ *and it looks like Fig. 3.*

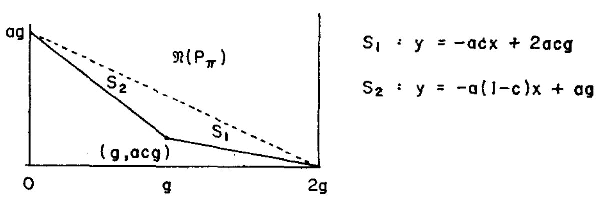


Figure 3

(c) *If the Newton polygon $\mathfrak{N}(P_\pi)$ has the shape as (Fig. 3), then the p-divisible group $J(p)$ of $J(C)$ is isogenous to $t(G_{n_c,m_c} + G_{m_c,n_c})$ where n_c, m_c are positive integers such that $1 \leqslant n_c < m_c$, $(n_c, m_c) = 1$, and $n_c + m_c = d =$: the number of distinct characteristic roots τ_i of $P_\pi(\lambda)$ with $\nu_p(\tau_i) = ac$, $0 < c < \frac{1}{2}$, and $td = g$. In other words, $\mathfrak{N}(P_\pi)$ determines the isotypic components of $J(p)$ (rather than its simple components).*

DEFINITION 6.1. The formal group of the type $G_{n,m} + G_{m,n}$ where n, m are positive integers such that $1 \leqslant n < m$, $(n, m) = 1$, and $n + m = g$ is called *the symmetric formal group of dimension g.*

Proof of Theorem 6.1. (a) (ai) $\Rightarrow$ (aii). Put $p^a/\tau_i = \tau_{g+i}$ for $i = 1,\ldots, g$. Then $\nu_p(\tau_i) = ac$, $\nu_p(\tau_{g+i}) = a(1-c)$ for every $1 \leqslant i \leqslant g$, from which we have immediately that $v_p(a_{2g}) = 0$, $v_p(a_{2g-i}) \geqslant aci$ for every $1 \leqslant i \leqslant g$, $v_p(a_g) = acg$, and $v_p(a_{g-i}) \geqslant acg + ia(1-c)$ for every $1 \leqslant i \leqslant g$. Hence it follows that

$$\frac{v_p(a_{2g-i})}{ai} \geqslant c, \qquad \frac{v_p(a_g)}{ag} = c, \qquad \text{and} \qquad \frac{v_p(a_{g-i})}{a(g+i)} \geqslant c.$$

Therefore, we get

$$\operatorname*{Min}_{0 \leqslant i \leqslant 2g} \frac{v_p(a_i)}{a(2g-i)} = \frac{v_p(a_g)}{ag} = c.$$

Now put $n_c = cg$ and $m_c = g - n_c = (1-c)g$. Then n_c, m_c are positive integers satisfying $1 \leqslant n_c < m_c$, $n_c + m_c = g$, $(n_c, m_c) = 1$, and $c = n_c/(n_c + m_c)$. (In fact, if $(n_c, m_c) \neq 1$, then $n_c = dn_c'$ with $n_c' = cg/d$. This implies that $P_\pi(\lambda)$ has g/d distinct roots with $\nu_p(\tau_i) = ac$, which contradicts to the hypothesis of (ai).)

(aii) $\Rightarrow$ (aiii). See Manin [6, Theorem 4.1′].

(aiii) $\Rightarrow$ (ai). Suppose that $P_\pi(\lambda)$ has no such decomposition as (ai). Then we have either

$$\operatorname{Min} \frac{v_p(a_i)}{a(2g-i)} = \frac{t_1}{t_2} \neq \frac{n_c}{n_c + m_c}$$

or

$$\operatorname{Min} \frac{v_p(a_i)}{a(2g-i)} = \frac{v_p(a_l)}{a(2g-l)} = \frac{n_c}{n_c + m_c} \qquad \text{for} \quad l > g.$$

In the first case, $J(p)$ is isogenous to the formal group of the type $G_{t_1,t_2-t_1} + G_{t_2-t_1,t_1}$ which is obviously nonisogenous to $G_{n_c,m_c} + G_{m_c,n_c}$. In the latter case, $J(p)$ is isogenous to $G_{n_c,m_c} + G_{m_c,n_c} + G'$ with dimension of $G' > 1$. But this is impossible, because $n_c + m_c + \dim G' > g$.

(b) The assertion follows immediately from the proof of (ai) $\Rightarrow$ (aii) and from the hypothesis $0 < c < \frac{1}{2}$.

(c) Corresponding to the segment S_1, we get g roots τ_i with $\nu_p(\tau_i) = ac$, $0 < c < \frac{1}{2}$ for every $1 \leqslant i \leqslant g$. If there are d distinct roots $\tau_1, \ldots, \tau_d$ among them, then $\prod_{i=1}^{d} (\lambda - \tau_i) \in \mathbb{Z}_p[\lambda]$ and $P_\pi(\lambda)$ has the p-adic decomposition as

$$P_\pi(\lambda) = \Bigg(\prod_{\substack{i=1 \\ \nu_p(\tau_i)=ac}}^{d} (\lambda - \tau_i)(\lambda - p^a/\tau_i) \Bigg)^{g/d}.$$

Hence $J(p)$ is isogenous to $t(G_{n_c', m_c'} + G_{m_c', n_c'})$ with $1 \leqslant n_c' < m_c'$, $(n_c', m_c') = 1$, and $m_c' + n_c' = d$. So $\mathfrak{N}(P_\pi)$ determine the isotypic component of $J(p)$. Q.E.D.

THEOREM 6.2. *Suppose that $J(C)$ is elementary and that the p-divisible group $J(p)$ of $J(C)$ is isogenous to the symmetric formal group of dimension g : $G_{n,m} + G_{m,n}$ $1 \leqslant n < m$, $(n, m) = 1$, and $n + m = g$. Then the following statements are equivalent:*

(i) *g divides the residue degree at every prime v in Φ lying over p.*

(ii) *$P_\pi(\lambda)$ is $\mathbb{Q}$-irreducible, but $P_\pi(\lambda) = P_{\nu_1}(\lambda)\, P_{\nu_2}(\lambda)$ where*

$$P_{\nu_1}(\lambda) = \prod_{\substack{i=1 \\ \nu_p(\tau_i)=an/g}}^{g} (\lambda - \tau_i) \text{ and } P_{\nu_2}(\lambda) = \prod_{\substack{i=1 \\ \nu_p(\tau_i)=am/g}}^{g} (\lambda - \tau_i) \text{ are } \mathbb{Q}_p\text{-irreducible.}$$

(iii) *$J(C)$ is k-simple.*

(iv) *$\mathscr{A} = \Phi = \mathbb{Q}(\pi)$ is a CM-field of degree $2g$. Φ has the imaginary quadratic field K_0 in which p splits.*

Proof. (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii). As $J(C)$ is elementary, $P_\pi(\lambda) = P(\lambda)^e$ with $P(\lambda)$ $\mathbb{Q}$-irreducible and $P(\pi) = 0$. Corresponding to the primes ν in $\Phi = \mathbb{Q}(\pi)$ over p, $P(\lambda)$ is decomposed into the product of $\mathbb{Q}_p$-irreducible factors $P_\nu(\lambda)$. Now we shall compute the local invariants of $\mathscr{A} = \mathrm{End}_k(J(C)) \otimes \mathbb{Q}$ at primes ν in $\Phi = \mathbb{Q}(\pi)$. First note that there are no real primes in Φ. Now by Manin [6], $P_\pi(\lambda)$ has the p-adic factorization in the ring $W(\bar{k})\,[p^{1/g}]$ where $W(\bar{k})$ denotes the ring of Witt vectors over $\bar{k}$, as

$$P_\pi(\lambda) = \prod_{i=1}^{g} (\lambda - p^{an/g} x_i) \cdot \prod_{i=1}^{g} (\lambda - p^{am/g} y_i),$$

where x_i, y_i are invertible elements in $W(\bar{k})\ [p^{1/g}]$. So $P_\nu(\lambda)$ splits in the ring $W(\bar{k})\,[p^{1/g}]$ into linear factors $(\lambda - p^{an/g} x_i)$, $(\lambda - p^{am/g} y_i)$. So the local invariants are

$$i_\nu = \mathrm{ord}_\nu(\pi) \cdot [\Phi_\nu : \mathbb{Q}_p]/a = \mathrm{ord}_\nu(\pi) \cdot f_\nu/a = \frac{(an/g) \cdot f_\nu}{a} \text{ or } \frac{(am/g) \cdot f_\nu}{a},$$

where f_ν is the residue degree at ν with $1 \leqslant f_\nu \leqslant g$. Hence $e = 1$, if and only if all the i_ν are integers, if and only if $P_{\nu_i}(\lambda)$, $i = 1, 2$ are $\mathbb{Q}_p$-irreducible, if and only if $f_{\nu_i} = g$ for $i = 1, 2$. This proves the equivalences (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii).

(ii) $\Rightarrow$ (iv). Since π is imaginary with $\deg(\pi) = 2g$, $\Phi = \mathbb{Q}(\pi)$ is a CM-field of degree $2g$. Corresponding to the p-adic decomposition (ii) of $P_\pi(\lambda)$, there are two valuations ν_1, ν_2 in Φ over p with $\operatorname{ord}_{\nu_1}(\pi) = an/g$ and $\operatorname{ord}_{\nu_2}(\pi) = am/g$. In other words, there are two prime ideals ν_1, ν_2 over p such that $(\pi^g) = \nu_1^{an}\nu_2^{am}$. Now the Riemann hypothesis $|\pi| = p^{a/2}$ implies that $(p) = \nu_1\nu_2$ and ν_1, ν_2 are complex conjugates. Since $f_{\nu_i} = g$ for $i = 1, 2$, p splits in an imaginary quadratic subfield K_0 of Φ, whence the assertion (iv).

(iv) $\Rightarrow$ (i). Suppose that the CM-field $\Phi = \mathbb{Q}(\pi)$ has an imaginary quadratic subfield K_0 in which p splits: $(p) = \nu\nu'$ where ν, ν' are complex conjugates. Take an ideal $\mathfrak{A}$ such that $\mathfrak{A}^g = \nu^{an}\nu'^{am}$ with $1 \leqslant n < m$, $(n, m) = 1$ and $n + m = g$. Then $\mathfrak{A}$ satisfies $\mathfrak{A}\mathfrak{A}' = (p^a)$ where $\mathfrak{A}'$ denotes the conjugate of $\mathfrak{A}$, and hence we can find an algebraic integer $\tau \in \Phi$ such that $(\tau) = \mathfrak{A}$ (cf. Honda [4]). Thus $(\tau^g) = \nu^{an}\nu'^{am}$ and $\operatorname{ord}_\nu(\pi) = an/g$, $\operatorname{ord}_{\nu'}(\pi) = am/g$, and we see that $P_\pi(\lambda)$ has g p-adic roots τ_i with order an/g together with g p-adic roots τ_i with order am/g. Hence the local invariants are $i_\nu \equiv (n/g) \cdot f_\nu$ and $(m/g) \cdot f_\nu \pmod{\mathbb{Z}}$. But the commutativity hypothesis of $\mathscr{A}$ implies that $i_\nu \equiv 0 \pmod{\mathbb{Z}}$. This holds true if and only if f_ν and $f_{\nu'}$ are divisible by g. Q.E.D.

Example 6.3. We again consider the curve $y^2 = 1 - x^7$ defined over the prime field $\mathbb{F}_p$ where p is a prime such that $p \equiv 2$ or $4 \pmod 7$. The Cartier–Manin matrix A of C is given by

$A = (c_{m,n})_{m,n=1,2,3}$ where for $p \equiv 2 \pmod 7$,

$$c_{1,2} = \binom{(p-1)/2}{(p-2)/7} \cdot (-1)^{(p-2)/7}, \; c_{m,n} = 0 \text{ otherwise},$$

and for $p \equiv 4 \pmod 7$,

$$c_{2,1} = \binom{(p-1)/2}{(2p-1)/7} \cdot (-1)^{(2p-1)/7}, \; c_{m,n} = 0 \text{ otherwise}.$$

So $|A| = 0$ and $A\,A^{(p)} = (0)$ in both cases.

Now it is easy to see that the primes $p \equiv 2$ or $4 \pmod 7$ satisfy $p^3 \equiv 1 \pmod 7$. So in the notations of Example 5.4, we have $f = 3$ and $r' = 2$. Hence p splits in the unique subfield $K_0 = \mathbb{Q}((-7)^{1/2})$ of $L = \mathbb{Q}(\zeta)$. Moreover, Honda [3] has shown that for any $s \geqslant 1$, $\mathbb{Q}(\pi^{3s}) = K_0$. Hence $2 \leqslant [\Phi : \mathbb{Q}] \leqslant 6$ and $[\mathscr{A} : \mathbb{Q}] \leqslant 3^2 \cdot 2$. As $\mathscr{A}$ contains the subfield $L = \mathbb{Q}(\zeta)$ of degree $2 \cdot 3$, $\mathscr{A}$ is a simple algebra over K_0. Now note that $K_0 = \mathbb{Q}((-7)^{1/2})$ has the basis $\{1, (1 + (-7)^{1/2})/2\}$.

So we have

$$\pi^3 = a_1 + a_2\left(\frac{1+(-7)^{1/2}}{2}\right), \qquad a_1, a_2 \in \mathbb{Z} \quad \text{with} \quad N(\pi^3) = p^3.$$

Hence the characteristic polynomial of π^3 is given by

$$P_{\pi^3}(\lambda) = (\lambda^2 - (2a_1 + a_2)\lambda + p^3)^3 =: Q(\lambda)^3,$$

where $Q(\lambda)$ is $\mathbb{Q}$-irreducible and $(2a_1 + a_2)^2 - 4p^3 = -7a_2^2 < 0$. Since p splits in K_0, the polynomial $Q(\lambda)$ must factor p-adicly, giving two primes ν_1, ν_2 with $\mathrm{ord}_{\nu_1}(\pi^3) = 1$ and $\mathrm{ord}_{\nu_2}(\pi^3) = 2$. Hence $\mathrm{ord}_{\nu_1}(\pi) = \frac{1}{3}$ and $\mathrm{ord}_{\nu_2}(\pi) = \frac{2}{3}$. Hence over some finite extension of $\mathbb{Q}_p$, $P_\pi(\lambda)$ has three roots τ_i with the order $\frac{1}{3}$ and hence we get $n_{1/3} = 1$, $m_{1/3} = 3 - 1 = 2$. So $J(p)$ is isogenous to $G_{1,2} + G_{2,1}$.

What is the algebraic structure of $J(C)$? First we know that there are no real primes in Φ. The local invariants are $i_\nu = 1, 2$ and hence $\mathscr{A}$ is commutative with $[\mathscr{A} : \mathbb{Q}] = 6$. Thus $J(C)$ is simple over $\mathbb{F}_p$.

7. The Jacobian Variety $J(C)$ of C with the Formal Structure of Mixed Types

THEOREM 7.1. *Suppose that the Cartier–Manin matrix A of C is such that $A \neq (0)$, but $|A| = 0$ in k. Let $|A_\pi - \lambda I_g| = \sum_{i=0}^{g} b_i\lambda^i$, $b_g = 1$ be the characteristic polynomial of $A_\pi = A\,A^{(p)} \cdots A^{(p^{a-1})}$. Then we have*

(a) *The following statements are equivalent*:

(ai) *There is an integer $1 < t < g$ such that $(b_t, p) = 1$ and $b_j \equiv 0 \pmod p$ for all $j = 0, \ldots, t-1$.*

(aii) *There exist the polynomials $P_0(\lambda)$, $P_a(\lambda)$, and $g(\lambda)$ over $\mathbb{Z}_p$ such that $P_0(\lambda) = \prod_{i=1}^{g-t}(\lambda - \tau_i)$, $P_a(\lambda) = \prod_{i=1}^{g-t}(\lambda - p^a/\tau_i)$ with $\nu_p(\tau_i) = 0$ for every $1 \leqslant i \leqslant g - t$, $g(\lambda) \equiv \lambda^{2t} \pmod p$ and that $P_\pi(\lambda) = P_0(\lambda)\,P_a(\lambda)\,g(\lambda)$.*

(aiii) *The p-divisible group $J(p)$ of $J(C)$ has the component $(g-t)G_{1,0}$. The formal group Γ of $J(C)$ has height $g + t$.*

(aiv) *The p-rank of $J(C)$ is $g - t$.*

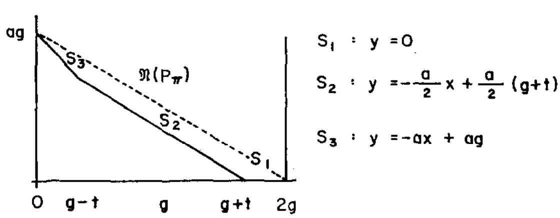


FIGURE 4

(b) *Assume that* (a) *is true*; *then the following statements are equivalent*:

(bi) $g(\lambda) = \prod_{i=1}^{2t} (\lambda - \tau_i)$ *with* $v_p(\tau_i) = a/2$ *for every* $1 \leqslant i \leqslant 2t$.

(bii) *The Newton polygon* $\mathfrak{N}(P_\pi)$ *of* $P_\pi(\lambda)$ *has the shape of Fig.* 4.

When the above is true, the p-divisible group $J(p)$ *of* $J(C)$ *is isogenous to* $(g - t)G_{1,0} + tG_{1,1}$ *and* $\mathbf{\Gamma}$ *to* $G_m(p)^{g-t} + tG_{1,1}$.

(c) *Assume that* (a) *is true*; *then the following statements are equivalent*:

(ci) $g(\lambda) = \prod_{i=1}^{t} (\lambda - \tau_i)(\lambda - p^a/\tau_i)$ *with* τ_i *simple roots but* $v_p(\tau_i) = ac$, $0 < c < \frac{1}{2}$ *for every* $1 \leqslant i \leqslant t$.

(cii) *Write* $g(\lambda) = \sum_{i=0}^{2t} d_i\lambda^i$. *Then* $g(\lambda)$ *is a distinguished polynomial over* $\mathbb{Z}_p$ *and the coefficients* d_i *satisfy the conditions*:

$$\underset{0 \leqslant i \leqslant 2t}{\mathrm{Min}} \frac{v_p(d_i)}{a(2t - i)} = \frac{v_p(d_t)}{at} = \frac{n}{n + m},$$

where n, m are positive integers satisfying $1 \leqslant n < m$, $(n, m) = 1$, *and* $n + m = t$.

(ciii) *The p-divisible group* $J(p)$ *of* $J(C)$ *is isogenous to* $(g - t)G_{1,0} + G_{n,m} + G_{m,n}$ *where n, m are positive integers satisfying* $1 \leqslant n < m$, $(n, m) = 1$ *and* $n + m = t$, *and* $\mathbf{\Gamma}$ *to* $G_m(p)^{g-t} + G_{n,m} + G_{m,n}$.

When the above is true, the Newton polygon $\mathfrak{N}(P_\pi)$ *of* $P_\pi(\lambda)$ *has the shape of Fig.* 5.

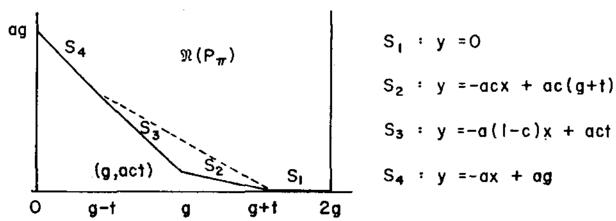


FIGURE 5

Proof. (a) (ai) $\Rightarrow$ (aii). Assume (ai). Then

$$P_\pi(\lambda) \equiv (-1)^{g+t}\lambda^{g+t} \{(-1)^{g-t}\lambda^{g-t} + \cdots + b_t\} \pmod{p},$$

where λ^{g+t} and $(-1)^{g-t}\lambda^{g-t} + \cdots + b_t$ are relatively prime. So by Hensel's lemma, there exist polynomials $P_0(\lambda)$, $h(\lambda)$ over $\mathbb{Z}_p$ such that

$$\begin{aligned} P_0(\lambda) &\equiv (-1)^{g-t}\lambda^{g-t} + \cdots + b_t \quad \pmod{p}, \quad \deg P_0(\lambda) = g - t, \\ h(\lambda) &\equiv (-1)^{g+t}\lambda^{g+t} \quad \pmod{p}. \end{aligned}$$

Moreover, in the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, $P_0(\lambda) = \prod_{i=1}^{g-t} (\lambda - \tau_i)$ with $v_p(\tau_i) = 0$ for every $1 \leqslant i \leqslant g - t$, because b_t is a p-adic unit. Since $P_\pi(\lambda)$ has always together with a root τ_i, the root p^a/τ_i, $h(\lambda)$ contains the factor

$P_a(\lambda) = \prod_{i=1}^{g-t} (\lambda - p^a/\tau_i)$ with $\nu_p(\tau_i) = 0$ for every $1 \leqslant i \leqslant g - t$. So there exists $g(\lambda) \in \mathbb{Z}_p[\lambda]$ such that $g(\lambda) \equiv (-1)^{2t}\lambda^{2t} \pmod p$ and that $h(\lambda) = P_a(\lambda)\, g(\lambda)$.

(aii) $\Rightarrow$ (aiii). The first part follows from the Manin theorem 4.1 in [6]. The formal group $\mathbf{\Gamma}$ of $J(C)$ is the connected component $J(p)/(\mathbb{Q}_p/\mathbb{Z}_p)_k^{g-t}$ of $J(p)$, whence it has height $2g - (g - t) = g + t$.

(aiii) $\Rightarrow$ (aiv). This follows from the fact that the p-rank of $J(C)$ coincides with the rank of the component $G_{1,0}$ in $J(p)$.

(aiv) $\Rightarrow$ (ai). The Dieudonné module corresponding to the $J(p)$ contains the factors $T_p(G_m(p)^{g-t}) \oplus T_p((\mathbb{Q}_p/\mathbb{Z}_p)_k^{g-t})$. Hence we can write $P_\pi(\lambda) = P_a(\lambda)\ P_0(\lambda)\ g(\lambda)$ where $P_a(\lambda)$ (resp. $P_0(\lambda)$: resp. $g(\lambda)$) is the characteristic polynomial of the restriction of the p-adic representation $T_p(\pi)$ of the Frobenius endomorphism π to $T_p(G_m(p)^{g-t})$ (resp. $T_p((\mathbb{Q}_p/\mathbb{Z}_p)_k^{g-t})$: resp. $T_p(J(p)/(g - t)G_{1,0})$). Both $P_a(\lambda)$ and $P_0(\lambda)$ have the same degree $g - t$ and moreover, $P_0(\lambda) = \prod_{i=1}^{g-t} (\lambda - \tau_i)$ with $\nu_p(\tau_i) = 0$ for every $1 \leqslant i \leqslant g - t$, since $(\mathbb{Q}_p/\mathbb{Z}_p)_k$ is étale. As $P_\pi(\lambda)$ satisfies the congruence (4) in Section 3:

$$P_\pi(\lambda) \equiv (-1)^g\lambda^g \mid A_\pi - \lambda I_g \mid \pmod p,$$

we have $\mid A_\pi - \lambda I_g \mid \equiv \lambda^t P_0(\lambda) \pmod p$. Here take $b_t \equiv P_0(0) \pmod p$. Then $(b_t, p) = 1$ and $b_j \equiv 0 \pmod p$ for all $j = 0,..., t - 1$.

(b) (bi) $\Rightarrow$ (bii). Putting $P_\pi(\lambda) = P_0(\lambda)\, P_a(\lambda)\, g(\lambda) = \sum_{i=0}^{2g} a_i\lambda^i$, we have immediately that $v_p(a_{2g-i}) = 0$ for every $0 \leqslant i \leqslant g - t$, $v_p(a_{g+t-i}) = (a/2)i$ for every $1 \leqslant i \leqslant 2t$, $v_p(a_{g-t-i}) = a(t + i)$ for every $1 \leqslant i \leqslant g - t$. Hence the Newton polygon $\mathfrak{N}(P_\pi)$ of $P_\pi(\lambda)$ has the segments S_1, S_2, S_3 with slopes 0, $-a/2$ and $-a$, respectively, and looks like Fig. 4.

(bii) $\Rightarrow$ (bi). Any segment $(j, v_p(a_j)) \leftrightarrow (l, v_p(a_l))$ with $l > j$ of $\mathfrak{N}(P_\pi)$ with slope $-m$ gives the roots $\tau_1, ..., \tau_{l-j}$ of $P_\pi(\lambda)$ in $\bar{\mathbb{Q}}_p$ with $\nu_p(\tau_i) = m$ for every $1 \leqslant i \leqslant l - j$. Moreover, $\prod_{i=1}^{l-j} (\lambda - \tau_i)$ with $\nu_p(\tau_i) = m$, is in $\mathbb{Z}_p[\lambda]$ and divides $P_\pi(\lambda)$. Hence the segments S_1, S_2, and S_3 correspond respectively to the factors $P_0(\lambda)$, $g(\lambda)$, and $P_a(\lambda)$. Therefore, the p-divisible group $J(p)$ is isogenous to $(g - t)\, G_{1,0} + tG_{1,1}$, and $\mathbf{\Gamma}$ to $G_m(p)^{g-t} + tG_{1,1}$.

(c) Since $g(\lambda)$ is the characteristic polynomial of the restriction of $T_p(\pi)$ to the Dieudonnλ module $T_p(J(p)/(g - t)G_{1,0})$, we have $g(\lambda) = \prod_{i=1}^{t} (\lambda - \tau_i)\ (\lambda - p^a/\tau_i)$ with $0 < \nu_p(\tau_i) < a/2$. Hence the same proof as Theorem 6.1a for $g(\lambda)$ yield the equivalences (ci) $\Leftrightarrow$ (cii) $\Leftrightarrow$ (ciii).

Now the factorization $P_\pi(\lambda) = \sum_{i=0}^{2g} a_i\lambda^i = P_0(\lambda)\, P_a(\lambda)\, g(\lambda)$ gives $v_p(a_{2g-i}) = 0$ for every $0 \leqslant i \leqslant g - t$, $v_p(a_{g+t-i}) \geqslant aci$ for every $1 \leqslant i < t$, $v_p(a_g) = act$ and $v_p(a_{g-i}) \geqslant act + a(1 - c)i$ for every $1 \leqslant i < t$, $v_p(a_{g-t}) = at$ and $v_p(a_{g-t-i}) \geqslant a(t + i)$ for every $1 \leqslant i \leqslant g - t$. Hence the Newton polygon $\mathfrak{N}(P_\pi)$ has the segments S_i, $i = 1,..., 4$ with slopes 0, $-ac$, $-a(1 - c)$, and $-a$, respectively, and looks like Fig. 5. Q.E.D.

THEOREM 7.2. *Let π be a Weil number of order a and suppose that the center $\Phi = \mathbb{Q}(\pi)$ of $\mathscr{A} = \mathrm{End}_k(J(C)) \otimes \mathbb{Q}$ is a CM-field of degree 2g. Put $\beta = \pi + \bar{\pi} = \pi + p^a/\pi$. Then we have*

(a) *$J(C)$ is elementary.*

(b) $P_\pi(\lambda) = \lambda^2 - \beta\lambda + p^a \in \mathbb{Q}(\beta)[\lambda]$. Moreover, we have

(b1) *$(\beta, p) = 1 \Leftrightarrow J(C)$ is ordinary.*

(b2) *Assume that $(\beta, p) \neq 1$ and let $f(\lambda) = \sum_{i=0}^{g} d_i\lambda^i$, $d_g = 1$ be the minimal polynomial of β. Then we have*

(b2.1) *If $\beta = \pm p^{a/2}\alpha$ with α an algebraic integer satisfying $(Norm(\alpha), p) = 1$, then $J(C)$ is supersingular.*

(b2.2) *If there exists the integer t such that $(d_t, p) = 1$, but $d_j \equiv 0 \pmod p$ for every $1 \leqslant j < t$ (take the smallest t if there are more than one such integers), then the p-divisible group $J(p)$ contains the component $(g - t)G_{1,0}$. Moreover, if there is a valuation ν over p in $\mathbb{Q}(\beta)$ such that $ord_\nu(\beta) = a/2$ and that ν is unramified in Φ, then the p-divisible group $J(p)$ is isogenous to $(g - t)G_{1,0} + tG_{1,1}$, but $J(C)$ is k-simple.*

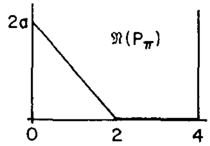
Proof. (a) This is the main theorem of Honda [4].

(b) For (b1), see Theorem 3.2 and for (b2.1), see Theorem 5.2.

(b2.2) It follows from the hypothesis that $f(\lambda) \equiv \lambda^t(\lambda^{g-t} + \cdots + d_t) \pmod p$. Hence $f(\lambda)$ gives $(g - t)$ p-adic roots with order 0. At these places ν, we have $\mathrm{ord}_\nu(\beta) = 0$ and the equation $\lambda^2 - \beta\lambda + p^a = 0$ must split, giving roots of orders 0 and a. Hence the local invariants i_ν are integers, so satisfies the commutativity condition for $\mathscr{A}$. This argument also shows that the p-divisible group $J(p)$ contains the component $(g - t)G_{1,0}$. Now we have a distinguished polynomial over $\mathbb{Z}_p$ corresponding to the factor λ^t of $f(\lambda)$ modulo p. Suppose that there is a valuation ν_2 in $\mathbb{Q}(\beta)$ over p such that $\mathrm{ord}_{\nu_2}(\beta) = a/2$. Then we may write $\beta = \pm p^{a/2}\alpha$ with α an invertible element in $\mathbb{Q}_p(\beta)$ such that $(\alpha, p) = 1$. The equation $\lambda^2 - \beta\lambda + p^a = 0$ gives $\pi = p^{a/2}Y$ where Y satisfies the equation $Y^2 - \alpha Y + 1 = 0$. In modulo ν_2 (i.e., in $\mathbb{F}_p$, since ν_2 is ramified) if $Y^2 - \alpha Y + 1 = 0$ has no solution, then it must be irreducible over $\mathbb{Q}_p(\beta)$. Hence Y generates an unramified quadratic extension over $\mathbb{Q}_p(\beta)$ and hence we get the unique extension of ord_{ν_2} to $\Phi = \mathbb{Q}(\pi)$ with residue degree 2. So π has $\mathrm{ord}_{\nu_2}(\pi) = a/2$ for the unique extension (again denoted) ord_{ν_2} in Φ over ord_{ν_2}. This shows that $P_\pi(\lambda)$ has $2t$ p-adic roots with order $a/2$ and hence $J(p)$ contains the factor $tG_{1,1}$. Thus $J(p)$ is isogenous to $(g - t)G_{1,0} + tG_{1,1}$. Now we compute the local invariant i_{ν_2}; $i_{\nu_2} = ((a/2) \cdot 2)/a \in \mathbb{Z}$. Hence $\mathscr{A} = \Phi$ with $[\mathscr{A} : \mathbb{Q}] = 2g$ and hence $J(C)$ is k-simple. Q.E.D.

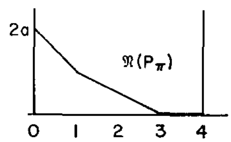
EXAMPLE 7.3. For hyperelliptic curves C of genus 2 over k, we have more complete classification theorem for the p-divisible group $J(p)$ of $J(C)$. The notation in Theorem 7.2 remains in force.

(a) $|A| \neq 0 \Leftrightarrow (\beta, p) = 1 \Leftrightarrow$



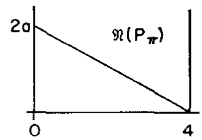
$\Leftrightarrow J(p) \sim 2G_{1,0} \Leftrightarrow J(C)$ is ordinary.

(b) $[|A| = 0$, but $A\ A^{(p)} \neq 0] \Leftrightarrow [(\beta, p) \neq 1$, but $(\mathrm{Tr}(\beta), p) = 1] \Leftrightarrow$



$\Leftrightarrow J(p) \sim G_{1,0} + G_{1,1}$.

(c) $[|A| = 0$ and $A\ A^{(p)} = (0)] \Leftrightarrow [(\beta, p) \neq 1$, $(\mathrm{Tr}(\beta), p^{a/2}) \neq 1$ and $(\mathrm{Norm}(\beta), p^a) \neq 1] \Leftrightarrow (\beta, p^{a/2}) \neq 1 \Leftrightarrow$



$\Leftrightarrow J(p) \sim 2G_{1,1} \Leftrightarrow J(C)$ is supersingular.

Proof. β being a real quadratic over $\mathbb{Q}$ and $\beta = \xi + \eta(d)^{1/2}$ with $\xi, \eta \in \mathbb{Q}$, and d square free, we have $P_\pi(\lambda) = \lambda^2 - \beta\lambda + p^a \in \mathbb{Q}(\beta)[\lambda]$ and $P_\pi(\lambda) = \lambda^4 - \mathrm{Tr}(\beta)\lambda^3 + (2p^a + \mathrm{Norm}(\beta))\lambda^2 - \mathrm{Tr}(\beta)\, p^a\lambda + p^{2a} \in \mathbb{Q}[\lambda]$ and $|A_\pi| \equiv \mathrm{Norm}(\beta) \pmod p$. Hence the assertions follow immediately. Q.E.D.

EXAMPLE 7.4. We shall give an example of k-simple Abelian variety of dimension 2 equipped with the mixed type of formal structure $G_{1,0} + G_{1,1}$. Let $k = \mathbb{F}_{7^2}$ and let $\beta = 6 + (29)^{1/2}$ in $\mathbb{Q}((29)^{1/2})$. Then $|\beta| < 2 \cdot 7$ and $\pi^2 - \beta\pi + 7^2 = 0$ gives a Weil number of order 2 and $\Phi = \mathbb{Q}(\pi)$ is a CM-field of degree 4. Since $(\beta, 7) \neq 1$, the Abelian variety X determined by π, up to isogeny, is nonordinary. Then the minimal polynomial of β over $\mathbb{Q}$ is given by $f(\lambda) = \lambda^2 - 12\lambda + 7$ and $f(\lambda) \equiv \lambda(\lambda + 2) \pmod 7$. So there are two valuations over 7 in $\mathbb{Q}(\beta)$: $\mathrm{ord}_{\nu_1}(\beta) = 0$ and $\mathrm{ord}_{\nu_2}(\beta) = 1$. At ord_{ν_2}, $\lambda^2 - \beta\lambda + 7^2 = 0$ splits, giving roots with orders 0 and 2. Hence the p-divisible group $X(p)$ of X has the component $G_{1,0}$. At ord_{ν_2}, $7 \mid \beta$ in $\mathbb{Q}_7$ and hence $\lambda^2 - \beta\lambda + 7^2 = 0$ has the solution $\pi = 7 \cdot \alpha$ where α satisfies the equation $\alpha^2 - 3\alpha + 1 = 0$. This α

generates an unramified quadratic extension over $\mathbb{Q}_7$. So there is a unique extension (again denoted) ord_{ν_2} of ord_{ν_2} to Φ with $\mathrm{ord}_{\nu_2}(\pi) = 1$. Hence $X(p)$ is isogenous to $G_{1,0} + G_{1,1}$. The characteristic polynomial of π over $\mathbb{Q}$ is $P_\pi(\lambda) = \lambda^4 - 12\lambda + 105\lambda^2 - 588\lambda + 7^4$, which is easily seen to be $\mathbb{Q}$-irreducible. Thus X is k-simple. Q.E.D.

Acknowledgment

I would like to thank Knud Lønsted for helpful discussions and Academicin Ju. I. Manin for advice during the preparation of this paper.

References

1. P. Cartier, Questions de rationalité des divisours en géométrie algébrique, *Bull. Soc. Math. France* **86** (1958), 177–251.
2. H. Hasse and E. Witt, Zyklische unverzweigte Erweiterungkörper vom Primzahlgrade p, über einem algebraischen Funktionenkörper der Charakteristik p, *Monatsch. Math. Phys.* **43** (1936), 477–492.
3. T. Honda, On the Jacobian variety of the algebraic curve $y^2 = 1 - x^l$ over a field of characteristic $p > 0$, *Osaka J. Math.* **3** (1966), 189–194.
4. T. Honda, Isogeny classes of Abelian varieties over finite fields, *J. Math. Soc. Japan* **20** (1968), 83–95.
5. S. Lang, "Abelian Varieties," Interscience Tracts in Pure and Applied Mathematics, No. 7, Wiley–Interscience, New York, 1959.
6. Ju. I. Manin, The theory of commutative formal groups over fields of finite characteristic, *Russian Math. Surveys* **18** (1963), 3–90.
7. Ju. I. Manin, The Hasse–Witt matrix of an algebraic curves, *Amer. Math. Soc. Transl. Ser.* **45** (1965), 245–264.
8. Ju. I. Manin, On the theory of Abelian verieties over fields of finite characteristic, *Izv. Akad. Nauk SSSR Ser. Mat.* **26** (1962), 281–292 (Russian.)
9. F. Oort, Supersingular Abelian varieties, Copenhagen talk (1975).
10. H. Schmidt, Über die Automorphismen eines algebraischen Funktionenkörper von Primzahlcharakteristik, *J. Reine Angew. Math.* **179** (1938), 5–15.
11. P. Serre, Quelques propriétés des variétés abéliannes en caractéristique p, *Amer. J. Math.* **80** (1958), 715–739.
12. G. Shimura and Y. Taniyama, "Complex Multiplication of Abelian Varieties," Publications of the Mathematical Society of Japan (1961).
13. J. Tate, Endomorphisms of Abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.
14. J. Tate, p-Divisible groups, *in* "Proceedings of the Conference on Local Fields, NUFFIC Summer School (Driebergen, Netherlands, 1966)," pp. 158–183, Springer-Verlag, New York/Berlin.
15. W. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* (1969), 521–560.
16. N. Yui, On the Jacobian varieties of algebraic curves over fields of characteristic $p > 0$, University of Copenhagen Math. Institute Preprint Ser. No. 42 (1977).