92. *On the Jacobian Varieties of Davenport-Hasse Curves*

By Toshihiko YAMADA

Department of Mathematics, Osaka University

(Comm. by Kenjiro SHODA, M.J.A., June 12, 1967)

Let p be any prime number, and consider the Davenport-Hasse curves C_a defined by the equations

(1) $$y^p - y = x^{p^a-1} \qquad (a=1, 2, 3, \cdots)$$

over the prime field $GF(p)$. If we denote by θ a primitive $(p^a-1)(p-1)$-th root of unity in the algebraic closure of $GF(p)$, the map

(2) $$\sigma: (x, y) \to (\theta x, \theta^{p^a-1} y)$$

defines an automorphism of C_a, which generates a cyclic group G of order $(p^a-1)(p-1)$. In this note we shall investigate the following problems:

1. To determine the l-adic representation of the automorphism group G (Theorem 1).
2. The decomposition of the jacobian variety J_a of C_a into simple factors (Theorem 2,3).
3. To give explicitly generators of endomorphism algebra (Theorem 5).

Detailed proofs and other aspects of Davenport-Hasse curves will be published elsewhere.

The author thanks to Professor Morikawa for his kind encouragement.

1. If we put $z = y^{p-1}$, the curve C_a is birationally equivalent to a curve defined by the equation

(3) $$x^{(p^a-1)(p-1)} = z(z-1)^{p-1}.$$

The previous automorphism σ is given in this case by

(2)′ $$\sigma: (z, x) \to (z, \theta x).$$

Now the following lemma is easily proved.

Lemma 1. The smallest natural number f such that $p^f \equiv 1 \bmod. (p^a-1)(p-1)$ is equal to $a(p-1)$.

Owing to this lemma, θ belongs to the field $k = GF(p^{a(p-1)})$. So the algebraic function field $k(z, x)$ defined by the equation (3) is a Kummer extension over $k(z)$ of degree $(p^a-1)(p-1)$, whose Galois group G is generated by σ. We denote by $\mathfrak{p}_0, \mathfrak{p}_1$, the prime divisors of $k(z)$ which are the numerators of principal divisors (z), $(z-1)$ respectively, and by $\mathfrak{p}_\infty$, the denominator of (z). Then on account of the equation (3), every prime divisor of $k(z)$ other than $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\infty$ is not ramified in $k(z, x)$. We shall make the table of behavior of the $\mathfrak{p}_i$ $(i=0, 1, \infty)$ in $k(z, x)$, where the notation is as usual.

$k(z)$	$k(z, x)$	e	f	g
$\mathfrak{p}_0$	$\mathfrak{P}_0$	$(p^a-1)(p-1)$	1	1
$\mathfrak{p}_1$	$\mathfrak{P}_{1,1}, \cdots, \mathfrak{P}_{1,p-1}$	p^a-1	1	$p-1$
$\mathfrak{p}_\infty$	$\mathfrak{P}_\infty$	$(p^a-1)(p-1)$	1	1

Since the prime divisors $\mathfrak{P}_0$, $\mathfrak{P}_{1,i}(1\leqslant i\leqslant p-1)$, $\mathfrak{P}_\infty$ of $k(z, x)$ have their degrees equal to one, they correspond respectively to the points P_0, $P_{1i}(1\leqslant i\leqslant p-1)$, P_∞ of the curve C_a. Let P be a point of C_a and n a positive integer. Let $V_n(P)$ be the n-th ramification group of P in G in the meaning of Weil [3]. Then, because of this table, we have

$$\begin{aligned} &V_1(P_0)=V_1(P_\infty)=G \\ (4)\qquad &V_1(P_{1,i})=\{\sigma^\nu;\ \nu\equiv 0 \bmod.\ p-1\} \qquad (1\leqslant i\leqslant p-1) \\ &V_2(P_0)=V_2(P_\infty)=V_2(P_{1,i})=\{e\}. \end{aligned}$$

We denote by ξ_α the correspondences of C_a defined by the elements α of G. Then the ξ_α induce endomorphisms on the Tate group $T_l(J_a)$ of the jacobian variety J_a of C_a. So we have a representation of G in the field of l-adic numbers, which is also written as ξ_α. We denote by $a_P(\alpha)$, for $\alpha\neq e$, the multiplicity of $P\times P$ in the intersection $\Delta\cdot\xi_\alpha$, where Δ is the diagonal of $C\times C_a$. We shall quote the result of Weil [3].

Lemma 2. The trace of the representation ξ_α of G in $T_l(J_a)$ is given by the formula:

$$(5)\qquad \begin{aligned} &\mathrm{Tr}(\xi_\alpha)=2-\sum_P a_P(\alpha)\ \ (\alpha\neq e) \\ &\mathrm{Tr}(\xi_e)=2g \end{aligned}$$

where g is the genus of C_a and is equal to $(p^a-2)(p-1)2$.

From this lemma and (4), we can get

$$(6)\qquad \mathrm{Tr}(\xi_{\sigma^\nu})=\begin{cases} -(p-1) & \nu\equiv 0 \bmod.\ p-1\ \ (\sigma^\nu\neq e) \\ \ \ 0 & \nu\not\equiv 0 \bmod.\ p-1. \end{cases}$$

Let ψ be a generator of the character group G^* of G. Then we have

$$\mathrm{Tr}(\xi_\alpha)=\sum_{\mu=1}^{(p^a-1)(p-1)} c_\mu\psi^\mu(\alpha),$$

where the coefficients c_μ are calculated by the relations of orthogonality of characters:

$$c_\mu=\frac{1}{(p^a-1)(p-1)}\sum_{\alpha\in G}\psi^\mu(\alpha^{-1})\mathrm{Tr}(\xi_\alpha).$$

From (5), (6) we get

$$c_\mu=\begin{cases} 1 & \mu\not\equiv 0 \bmod.\ p^a-1 \\ 0 & \mu\equiv 0 \bmod.\ p^a-1. \end{cases}$$

Thus we obtain

Theorem 1. The l-adic representation ξ_α in $T_l(J_a)$ of the automorphism group G is the direct sum of the irreducible representations ψ^ν of multiplicity one, where ν runs from 1 to $(p^a-1)\cdot(p-1)$ except $\nu\equiv 0 \bmod. p^a-1$.

2. In the first place we shall summarize the fact about the prime ideal decompositions of characteristic roots of Frobenius endomorphism (Davenport-Hasse [1]). Let χ be a character of order p^a-1 of $GF(p^a)^*$. Then the characteristic roots of p^a-th endomorphism on J_a are

$$(7)\qquad \tau_j(\chi^t)=-\sum_{u\neq 0}\chi^t(u)\exp\left[\frac{2\pi ij}{p}\operatorname{tr}(u)\right]\qquad \begin{pmatrix} t=1,\cdots,p^a-2\\ j=1,\cdots,p-1\end{pmatrix}.$$

Hereafter we shall put $q=p^a$. We denote by K_n the field of the n-th roots of unity over the field $\boldsymbol{Q}$ of rational numbers. Then the $\tau_j(\chi^t)$ belong to $K_{p(q-1)}$. The automorphism group of K_{q-1} over $\boldsymbol{Q}$ is isomorphic to the group R of prime residue-classes mod. $q-1$. Denote by P the subgroup of R which is generated by $p \bmod. q-1$, and let ρ run through representatives of the factor group R/P: $R=\sum_\rho \rho P$. Then the prime ideal decompositions of p in K_{q-1} and $K_{p(q-1)}$ can be written as follows:

$$(p)=\prod_\rho \mathfrak{p}_\rho \quad\text{in } K_{q-1},\quad (p)=\prod_\rho \mathfrak{P}_\rho^{p-1}\quad \text{in } K_{p(q-1)}.$$

For the sake of simplicity, we put $\tau(\chi^t)=\tau_1(\chi^t)$. Then it is easy to see that

$$\tau(\chi^t)\rightarrow\chi^{-1}(j)\tau(\chi^t)=\tau j(\chi^t)\qquad (1\leqslant j\leqslant p-1)$$

by the automorphisms $\exp\left(\frac{2\pi i}{p}\right)\rightarrow\exp\left(\frac{2\pi i}{p}j\right)$ of $K_{p(q-1)}$ over K_{q-1}.

For a rational integer α, we denote by $\lambda(\alpha)=\alpha_0+\alpha_1 p+\cdots+\alpha_{a-1}p^{a-1}$ $(0\leqslant\alpha_i\leqslant p-1$, not all $\alpha_i=p-1)$ the smallest non-negative residue of $\alpha \bmod. q-1$, and put $\sigma(\alpha)=\alpha_0+\alpha_1+\cdots+\alpha_{a-1}$. Then the prime ideal decompositions are as follows:

$$(8)\qquad \begin{aligned} (\tau(\chi^t)) &=\prod_\rho \mathfrak{P}_\rho^{\sigma(\rho t)} &&\text{in } K_{p(q-1)},\\ (\tau(\chi^t)^{p-1}) &=\prod_\rho \mathfrak{p}_\rho^{\sigma(\rho t)} &&\text{in } K_{q-1}.\end{aligned}$$

We shall say that $\tau_j(\chi^t)$ and $\tau_i(\chi^s)$ are equivalent when there exist natural numbers n, m such that $\tau_j(\chi^t)^m$ and $\tau_i(\chi^s)^n$ are conjugate to each other as algebraic numbers. Then, this is an equivalence relation. Let J_a be isogenous to a product:

$$(9)\qquad J_a\sim A_1\times A_2\times\cdots\times A_h,\ A_i=B_i\times\cdots\times B_i\qquad (i=1,\cdots,h),$$

where the B_i are simple abelian varieties not isogenous to each other. Then the $A_i (i=1,\cdots,h)$ are in one-to-one correspondence to the equivalence classes of the $\tau_j(\chi^t)$ (Tate [2]).

The following lemma is easily checked.

Lemma 3. For $0<\alpha<p^a-1$ we have

i) $1 \leqslant \sigma(\alpha) \leqslant a(p-1)-1$,

ii) $\sigma(\alpha)=1$ if and only if $\alpha=p^i$ $(0 \leqslant i \leqslant a-1)$,

iii) $\sigma(\alpha)=a(p-1)-1$ if and only if $\alpha=p^a-1-p^i$ $(0 \leqslant i \leqslant a-1)$.

Suppose that t satisfies $(t, p^a-1)=d>1$, then $(\lambda(\rho t), p^a-1)=d$, and by this lemma $\sigma(\rho t)$ cannot take the value 1 nor the value $a(p-1)-1$ for any ρ. On account of this fact and the prime ideal decomposition (8) of $\tau(\chi^t)$, we can conclude the following

Proposition 1. If t satisfies $(t, p^a-1)>1$, then $\tau(\chi)$ and $\tau(\chi^t)$ are not equivalent.

Corollary. The set $\{\tau_j(\chi^\mu);(\mu,p^a-1)=1, 1 \leqslant \mu < p^a-1, 1 \leqslant j \leqslant p-1\}$ fills up just an equivalence class of the $\tau_j(\chi^t)$.

We denote by K the decomposition field of p in K_{q-1}, and put $\boldsymbol{Q}\tau(x)=\bigcap_{\mu=1}^{\infty} \boldsymbol{Q}(\tau(\chi)^\mu)$. Then from lemma 3, we are able to see that $\boldsymbol{Q}_{\tau(\chi)}$ contains K. To show that the converse is also true, we need the following lemma which can be deduced from the expression of $\tau(\chi)$ as a Gaussian sum.

Lemma 4. $\tau(\chi)$ is invariant under the automorphisms $\exp \frac{2\pi i}{q-1} \longrightarrow \exp \frac{2\pi i}{q-1} p^i$ $(i=1, \cdots, a)$ of $K_{p(q-1)}$ over K_p.

After all we can reach at the equality:

$$\boldsymbol{Q}_{\tau(\chi)}=\boldsymbol{Q}(\tau(\chi)^{p-1})=K. \tag{10}$$

Now in the expression (9) of J_a as a product, let A_1 correspond to the equivalence class, to which $\tau(\chi)$ belongs (Prop. 1, Coroll.). Hereafter we put $A=A_1$. By virtue of what has been outlined, we may apply results of Tate [2] to our case.

Proposition 2. i) The endomorphism algebra $\mathcal{A}_0(A)$ of A is a central simple algebra over K, which splits at all finite primes of K not dividing p.

ii) The local invariants of $\mathcal{A}_0(A)$ at the primes $\mathfrak{p}_\rho$ are given by

$$\mathrm{inv}_{\mathfrak{p}_\rho}[\mathcal{A}_0(A)] \equiv \frac{\sigma(\rho)}{a(p-1)} \bmod. \boldsymbol{Z}.$$

iii) The dimension of the simple constituent B of A is $\dim B = (p-1)\cdot\varphi(p^a-1)/2$.

From Proposition 2, iii), we know that A is a simple abelian variety. Hence we have

Theorem 2. The jacobian variety J_a of the curve C_a contains as simple component the simple abelian variety A with multiplicity one, which has $\tau(\chi)^{p-1}$ as a characteristic root of the $p^{a(p-1)}$-th endomorphism. (We may say that A is the main component of J_a.)

As for the problem of the complete decomposition of J_a into simple factors, we can prove the following

Theorem 3. For $a=1$, we have

$$J_1 \sim \prod_t (B_t \times \cdots \times B_t) \qquad \text{(each } B_t \text{ appears } t \text{ times)}$$

where the index t runs over all divisors of $p-1$ except $t=p-1$, and each B_t is a simple abelian variety which has $\tau(\chi^t)$ as a characteristic root, and B_t is not isogenous to $B_{t'}$ for $t \neq t'$.

3. According to the notation of (9), the Tate group $T_l(J_a)$ is the direct sum of the Tate groups $T_l(A_i)$. Since the endomorphisms ξ_α of $T_l(J_a)$ induce endomorphisms $\xi_\alpha^{(i)}$ on each $T_l(A_i)$, the representation ξ_α on $T_l(J_a)$ of the automorphism group G of the curve C_a is the direct sum of the representations $\xi_\alpha^{(i)}$ on $T_l(A_i)$. Let as before $A=A_1$ be the main component of J_a. Then we have

Theorem 4. The representation $\xi_\alpha^{(1)}$ of G on $T_l(A)$ is the direct sum of the irreducible representations ψ^ν of multiplicity one, where ν runs through representatives of prime residue classes mod. $(p^a-1)(p-1)$.

Outline of proof. As $\mathcal{A}_0(A)$ is a division algebra, the characteristic roots of $\xi_\sigma^{(1)}$ are conjugate to each other. On the other hand the characteristic roots of ξ_σ are, by Theorem 1, $\{\psi^\nu(\sigma); \nu=1, \cdots, (p^a-1)(p-1), \nu \not\equiv 0 \text{ mod. } p^a-1\}$. From these facts and the equality $\varphi((p^a-1)(p-1))=(p-1)\cdot\varphi(p^a-1)=2\dim A$, the assertion may be deduced.

Corollary. $\boldsymbol{Q}(\xi_\sigma^{(1)})$ is the field $K_{(p^a-1)(p-1)}$ of $(p^a-1)(p-1)$-th roots of unity.

Although the structure of the algebra $\mathcal{A}_0(A)$ is determined by Proposition 2, we shall give generators of $\mathcal{A}_0(A)$ explicitly. The p-th endomorphism $\prod$ and the endomorphism ξ_σ of J_a induce endomorphisms of A, which are again denoted by $\prod$ and ξ_σ respectively. Let K denote the decomposition field of p in $\boldsymbol{Q}(\xi_\sigma)$, which is also the decomposition field of p in K_{p^a-1}. Then we can prove

Theorem 5. The endomorphism algebra $\mathcal{A}_0(A)$ of the main component A of J_a is the cyclic algebra over K:

$$(\textstyle\prod^{a(p-1)}, \boldsymbol{Q}(\xi_\sigma), \tau)$$

where σ is the automorphism of the curve C_a defined by (2), and τ is a generating automorphism of $\boldsymbol{Q}(\xi_\sigma)$ over K.

References

[1] H. Davenport and H. Hasse: Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. J. Reine Angew. Math., **172**, 151-182 (1935).

[2] J. Tate: Endomorphisms of abelian varieties over finite fields. Inventiones Math., **2**, 134-144 (1966).

[3] A. Weil: Sur les courbes algébriques et les variétés qui s'en déduisent. Paris, Hermann (1948).