J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

On the Davenport-Hasse curves

Dedicated to Professor Iyanaga on his 60th birthday

By Toshihiko YAMADA

(Received July 31, 1967)

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

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

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

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

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 Davenport-Hasse curves, on the basis of the automorphism groups G.

In § 1, we will determine the l-adic representation of G (Theorem 1).

In § 2, we shall investigate simple factors of the jacobian variety J_a of C_a. Let χ be a character of order p^a-1 of $GF(p^a)^*$. Then owing to Davenport-Hasse [1], the characteristic roots of p^a-th power endomorphism of J_a are

$$\tau_j(\chi^t) = -\sum_{u \in GF(p^a)^*} \chi^t(u) \exp\left[\frac{2\pi i j}{p} \mathrm{tr}\,(u)\right] \qquad \begin{pmatrix} t = 1, \cdots, p^a-2 \\ j = 1, \cdots, p-1 \end{pmatrix}. \tag{2}$$

Let J_a be isogenous to a product:

$$J_a \sim A_1 \times A_2 \times \cdots \times A_h,\ A_i = B_i \times \cdots \times B_i \qquad (i = 1, \cdots, h), \tag{3}$$

where the B_i are simple abelian varieties not isogenous to each other. Then the A_i are in one-to-one correspondence to the conjugate classes of the $\tau_j(\chi^t)$ as algebraic numbers (Tate [2]). Let $A = A_1$ correspond to the conjugate class of $\tau(\chi) = \tau_1(\chi)$, and call it the main component of J_a. Then we see that A is a simple abelian variety (Theorem 2). For $a = 1$, we describe completely the decomposition of the jacobian variety into simple factors (Theorem 3). The results are obtained from the prime ideal decomposition of the $\tau_j(\chi^t)$ and from determining the fields which are generated by the $\tau_j(\chi^t)$ over $\boldsymbol{Q}$, combined with the recent work of Tate [2].

In § 3, using results of § 1, the l-adic representation of the automorphism group G on the main component A is determined: the 'main' representation of G is realized on the main component A of J_a (Theorem 4). From this fact, we see that the endomorphism algebra $\mathcal{A}_0(A)$ of A is generated by the p-th power endomorphism and the endomorphism ξ_σ, which is induced by the automorphism σ defined by (1) (Theorem 5).

The author thanks to Professor H. Morikawa for his kind encouragement.

A short summary of this paper has been announced in [4].

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

$$x^{(p^a-1)(p-1)}=z(z-1)^{p-1}\,. \tag{4}$$

The previous automorphism σ is given in this case by

$$\sigma:(z,x)\longrightarrow(z,\theta x)\,. \tag{1$'$}$$

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

PROOF. For any non-negative integers ν, μ, we have

$$p^{a\nu+\mu}\equiv\nu p^a+p^\mu-\nu \qquad \text{mod. } (p^a-1)(p-1)\,.$$

Therefore, $p^{a\nu+\mu}\equiv 1$ mod. $(p^a-1)(p-1)$ $(0\leqq\mu<a)$, if and only if $\nu\equiv 0$ mod. $p-1$ and $\mu=0$. q. e. d.

By this lemma, θ is in the field $k=GF(p^{a(p-1)})$. So the algebraic function field $k(z,x)$ defined by the equation (4) 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). It is easy to see that $\mathfrak{p}_0$ and $\mathfrak{p}_\infty$ are totally ramified, and $\mathfrak{p}_1$ is ramified by exponent p^a-1, in $k(z,x)$. If we put $x^{p^a-1}(z-1)^{-1}=w$, the inertia field of $\mathfrak{p}_1$ in $k(z,x)$ is $k(z,w)$, of defining equation $w^{p-1}=z$. So $\mathfrak{p}_1$ decomposes in $k(z,w)$ into $p-1$ prime divisors. Summarizing, we have

$$\mathfrak{p}_0=\mathfrak{P}_0^{(p^a-1)(p-1)},\quad \mathfrak{p}_1=(\mathfrak{P}_{1,1}\cdots\mathfrak{P}_{1,p-1})^{p^a-1},\quad \mathfrak{p}_\infty=\mathfrak{P}_\infty^{(p^a-1)(p-1)} \tag{5}$$

in $k(z,x)$. Since the prime divisors $\mathfrak{P}_0$, $\mathfrak{P}_{1,i}$ $(1\leqq i\leqq p-1)$, $\mathfrak{P}_\infty$ are of degree one, they correspond respectively to the points P_0, $P_{1,i}$ $(1\leqq i\leqq p-1)$, P_∞ of the complete non-singular model C_a of the function field $k(z,x)$.

We denote by ξ_α, the correspondence of the curve C_a defined by an element α of the Galois group G. Let P be a point of C_a, and n a positive integer, and $\varDelta$ the diagonal of $C_a\times C_a$. We denote by $V_n(P)$ the subgroup of G composed of the identity element ε of G and of all the elements α of G, other than ε, such that $P\times P$ has in the intersection $\xi_\alpha\cdot\varDelta$ a coefficient which is at least equal to n. Then on account of (5), we have

$$V_1(P_0)=V_1(P_\infty)=G\,,\qquad\qquad (6)$$
$$V_1(P_{1,i})=\{\sigma^\nu;\ \nu\equiv 0 \text{ mod.}\, p-1\}\qquad (1\leqq i\leqq p-1)\,.$$

Since the ramification exponents are all prime to p, we have

$$V_2(P_0)=V_2(P_\infty)=V_2(P_{1,i})=\{\varepsilon\}\,.\qquad\qquad (7)$$

We denote by $M_l(\xi_\alpha)$ ($\alpha\in G$) the representation of G on the Tate group $T_l(J_a)$ of the jacobian variety J_a of C_a, where l is a prime number different from characteristic p, and denote by $a_P(\alpha)$ for $\alpha\neq\varepsilon$, the multiplicity of $P\times P$ in the intersection $\Delta\cdot\xi_\alpha$. We shall quote the result of Weil [3].

LEMMA 2. *The trace of the representation $M_l(\xi_\alpha)$ is given by the formula:*

$$\operatorname{tr} M_l(\xi_\alpha)=2-\sum_P a_P(\alpha)\qquad (\alpha\neq\varepsilon)\qquad\qquad (8)$$
$$\operatorname{tr} M_l(\xi_\varepsilon)=2g$$

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

From this lemma combined with (6) and (7), we calculate readily:

$$\operatorname{tr} M_l(\xi_{\sigma^\nu})=\begin{cases} -(p-1) & \nu\equiv 0 \text{ mod.}\, p-1 \quad (\sigma^\nu\neq\varepsilon)\\ 0 & \nu\not\equiv 0 \text{ mod.}\, p-1\,.\end{cases}\qquad\qquad (9)$$

As G is a cyclic group of order $(p^a-1)(p-1)$, its character group G^* is generated by ψ such that

$$\psi(\sigma^\nu)=\exp\frac{2\pi i\nu}{(p^a-1)(p-1)}\,.\qquad\qquad (10)$$

Then we have

$$\operatorname{tr} M_l(\xi_\alpha)=\sum_{\mu=1}^{(p^a-1)(p-1)} c_\mu\psi^\mu(\alpha)\,,$$

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

$$c_\mu=\frac{1}{(p^a-1)(p-1)}\sum_{\alpha\in G}\psi^\mu(\alpha^{-1})\operatorname{tr}M_l(\xi_\alpha)\,.$$

If we substitute the terms in the summation by (8), (9) and (10), we get

$$\begin{aligned} c_\mu&=\frac{1}{(p^a-1)(p-1)}\Big[2g-\sum_{\nu=1}^{p^a-2}\psi^\mu(\sigma^{-(p-1)\nu})\cdot(p-1)\Big]\\ &=\frac{1}{p^a-1}\Big[(p^a-2)-\sum_{\nu=1}^{p^a-2}\exp\frac{-2\pi i}{p^a-1}\mu\nu\Big]\\ &=\begin{cases} 1 & \mu\not\equiv 0 \quad \text{mod.}\, p^a-1\\ 0 & \mu\equiv 0 \quad \text{mod.}\, p^a-1\,.\end{cases}\end{aligned}$$

Thus we have proved

$$\operatorname{tr} M_l(\xi_\alpha) = \sum_{\nu \not\equiv 0 \bmod. p^\alpha - 1} \psi^\nu(\alpha)\,.$$

THEOREM 1. *The l-adic representation $M_l(\xi_\alpha)$ of the automorphism group G is the direct sum of the irreducible representations ψ^ν of multiplicity one, where ν runs from 1 to $(p^\alpha-1)(p-1)$ except $\nu \equiv 0$ mod. $p^\alpha-1$.*

§ **2.** In the first place we shall summarize the facts about the prime ideal decomposition of the characteristic roots $\tau_j(\chi^t)$ of p^α-th power endomorphism (Davenport-Hasse [**1**]). After this we put $p^\alpha = q$, and denote by K_n the field of the n-th roots of unity over the field $\boldsymbol{Q}$ of rational numbers. Then the $\tau_j(\chi^t)$ are in $K_{p(q-1)}$. We write simply $\tau(\chi^t)$ in place of $\tau_1(\chi^t)$. From the expression (2) of $\tau_j(\chi^t)$ it follows that

$$\tau(\chi^t) \longrightarrow \chi^{-t}(j)\tau(\chi^t) = \tau_j(\chi^t) \qquad (1 \leqq j \leqq p-1) \tag{11}$$

by the automorphisms $\exp \frac{2\pi i}{p} \to \exp \frac{2\pi i}{p} j$ of $K_{p(q-1)}$ over K_{q-1}, and

$$\tau(\chi^t) \longrightarrow \tau(\chi^{t\gamma}) \qquad ((\gamma, q-1) = 1) \tag{12}$$

by the automorphisms $\exp \frac{2\pi i}{q-1} \to \exp \frac{2\pi i}{q-1} \gamma$ of $K_{p(q-1)}$ over K_p. The Galois 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 mod. $q-1$, and let ρ run through representatives of the factor group R/P: $R = \sum_\rho \rho P$. Then the prime ideal decomposition of p is as follows:

$$(p) = \prod_\rho \mathfrak{p}_\rho \text{ in } K_{q-1},\ \mathfrak{p}_\rho = \mathfrak{P}_\rho^{p-1},\ (e^{\frac{2\pi i}{p}} - 1) = \prod_\rho \mathfrak{P}_\rho\,,$$

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

For a rational integer α, we denote by $\lambda(\alpha) = \alpha_0 + \alpha_1 p + \cdots + \alpha_{a-1} p^{a-1}$ $(0 \leqq \alpha_i \leqq p-1$, not all $\alpha_i = p-1)$ the smallest non-negative residue of α mod. $q-1$, and put $\sigma(\alpha) = \alpha_0 + \alpha_1 + \cdots + \alpha_{a-1}$. The prime ideal decomposition of $\tau(\chi^t)$ in $K_{p(q-1)}$ is

$$(\tau(\chi^t)) = \prod_\rho \mathfrak{P}_\rho^{\sigma(t\rho)}\,. \tag{13}$$

For the $(p-1)$-th power of $\tau(\chi^t)$ which belongs to K_{q-1} by (11), the prime ideal decomposition in K_{q-1} is

$$(\tau(\chi^t)^{p-1}) = \prod_\rho \mathfrak{p}_\rho^{\sigma(t\rho)}\,. \tag{14}$$

It is said that $\tau_j(\chi^t)$ and $\tau_i(\chi^s)$ are equivalent when there exist natural numbers n, m such that $\tau_j(\chi^t)^n$ and $\tau_i\ (\chi^s)^m$ are conjugate algebraic numbers. Clearly this is an equivalence relation. If the jacobian variety J_a is isogenous over the algebraic closure of $GF(p)$ to a product in the same notation as (3):

$$J_a \sim A_1 \times A_2 \times \cdots \times A_h,\ A_i = B_i \times \cdots \times B_i\,, \tag{3}$$

then the A_i are in one-to-one correspondence to the equivalence classes of the $\tau_j(\chi^t)$ (Tate [2]).

The following lemma is easily proved.

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

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

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

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

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

PROOF. Suppose that t satisfies $(t, p^a-1) = d > 1$, then $(\lambda(\rho t), p^a-1) = d$, and by Lemma 3, $\sigma(\rho t)$ cannot take the value 1 nor the value $a(p-1)-1$ for any ρ. If we assume that there exist natural numbers n and m such that $\tau(\chi)^n$ and $\tau(\chi^t)^m$ are conjugate algebraic numbers, the prime ideal decomposition (13) shows that the sets $\{n \cdot \sigma(\rho)\,;\,\rho\}$ and $\{m \cdot \sigma(t\rho)\,;\,\rho\}$ are the same. But this contradicts the above mentioned fact.

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

The decomposition fields of p in K_{q-1} and in $K_{p(q-1)}$ are the same, which we denote by K. For any natural number μ the prime ideal decomposition of $\tau(\chi)^\mu$ in $K_{p(q-1)}$ is $(\tau(\chi)^\mu) = \prod_\rho \mathfrak{P}_\rho^{\sigma(\rho)\mu}$. Among the numbers $\sigma(\rho)\mu$, the number μ appears only once because of Lemma 3. Therefore $\boldsymbol{Q}(\tau(\chi)^\mu)$ contains K.

LEMMA 4. $\tau(\chi)$ *is invariant under the automorphisms* $\exp\dfrac{2\pi i}{q-1} \to \exp\dfrac{2\pi i}{q-1}p^j$ $(j = 1, 2, \cdots, a)$ *of* $K_{p(q-1)}$ *over* K_p, *i.e.*, $\tau(\chi) = \tau(\chi^p) = \cdots = \tau(\chi^{p^{a-1}})$.

PROOF. From the expression of $\tau(\chi)$ as a generalized Gaussian sum, it follows that

$$\begin{aligned} \tau(\chi^{p^j}) &= -\sum_{u \neq 0} \chi^{p^j}(u) \exp\Big[\frac{2\pi i}{p}\mathrm{tr}(u)\Big] \\ &= -\sum_{u \neq 0} \chi(u^{p^j}) \exp\Big[\frac{2\pi i}{p}\mathrm{tr}(u^{p^j})\Big] \\ &= \tau(\chi)\,, \end{aligned}$$

which proves the assertion.

As $\tau(\chi) \to \chi^{-1}(j)\tau(\chi)$ $(1 \leqq j \leqq p-1)$ by the automorphisms $\exp\dfrac{2\pi i}{p} \to \exp\Big(\dfrac{2\pi i}{p}j\Big)$ of $K_{p(q-1)}$ over K_{q-1}, $\boldsymbol{Q}(\tau(\chi)^{p-1})$ is contained in K_{q-1}. Further, by Lemma 4,

$\tau(\chi)^{p-1}$ is invariant under the automorphisms of the decomposition group of p in K_{q-1}. Hence $\boldsymbol{Q}(\tau(\chi)^{p-1})$ is contained in K. When we put $\boldsymbol{Q}_{\tau(\chi)}=\bigcap_{\mu=1}^{\infty}\boldsymbol{Q}(\tau(\chi)^{\mu})$, from what has been stated, we get

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

Now for any ρ, prime ideal $\mathfrak{p}_\rho$ of K_{q-1} is regarded as prime ideal of K, which is also denoted by $\mathfrak{p}_\rho$. Let $\|\tau(\chi)^{p-1}\|_{\mathfrak{p}_\rho}$ denote the normal absolute value of $\tau(\chi)^{p-1}$ at the prime $\mathfrak{p}_\rho$ of K. From (14) we have $\|\tau(\chi)^{p-1}\|_{\mathfrak{p}_\rho}=p^{-\sigma(\rho)}$. Recall that $\tau(\chi)^{p-1}$ is a characteristic root of $p^{a(p-1)}$-th power endomorphism. Putting $p^{a(p-1)}=q_0$, we have

$$\|\tau(\chi)^{p-1}\|_{\mathfrak{p}_\rho}=q_0^{-\frac{\sigma(\rho)}{a(p-1)}}.$$

In the expression (3) of J_a, let A_1 correspond to the equivalence class, to which $\tau(\chi)$ belongs (Prop. 1, Coroll.). Hereafter we put $A_1=A$. Let $\mathcal{A}(A)$ denote the endomorphism ring of the abelian variety A, and put $\mathcal{A}_0(A)=\mathcal{A}(A)\otimes\boldsymbol{Q}$. We have prepared all things to apply Tate's results [2] to our case.

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

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

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

iii) *The dimension of the simple constituent B_1 of A is*

$$\dim B_1=\frac{1}{2}a(p-1)\cdot\deg\tau(\chi)^{p-1}=\frac{1}{2}(p-1)\cdot\varphi(p^a-1),$$

where φ is as usual the Euler's function.

Since by Prop. 1, Coroll., $\dim A$ is equal to $\frac{1}{2}(p-1)\cdot\varphi(p^a-1)$, Prop. 2, iii) shows 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 power endomorphism.* (*We call A the main component of J_a.*)

In the case of $a=1$, the situation is very simplified.

THEOREM 3. *For $a=1$, we have*

$$J_1\sim\prod_m(B_m\times\cdots\times B_m)\qquad(\textit{each } B_m \textit{ appears } m \textit{ times})$$

where the index m runs over all divisors of $p-1$ except $m=p-1$, and each B_m is a simple abelian variety of dimension $\frac{1}{2}\cdot\frac{p-1}{m}\varphi\left(\frac{p-1}{m}\right)$, which has $\tau(\chi^m)$ as a characteristic root, and B_m is not isogenous to $B_{m'}$, for $m\neq m'$.

PROOF. We exclude the case characteristic $p=2$, because in that case, the curve C_1 is of genus 0. As $a=1$, we have

$$\tau_j(\chi^t)=-\sum_{u\in GF(p)^*}\chi^t(u)\exp\left(\frac{2\pi ij}{p}u\right), \tag{2'}$$

and

$$\tau(\chi^t)=\prod_\rho \mathfrak{P}_\rho^{\lambda(t\rho)} \tag{13'}$$

where ρ ranges over representatives of prime residue-classes mod. $p-1$. Let m and n be any divisors of $p-1$ except m or $n=p-1$. Assume that $\tau(\chi^m)^\mu$ and $\tau(\chi^n)^\nu$ are conjugate algebraic numbers, for some positive integers μ and ν. Then by (13)′, the set $\{\mu\cdot\lambda(m\rho)\,;\rho\}$ and the set $\{\nu\cdot\lambda(n\rho)\,;\rho\}$ are the same. Since g. c. m. of the sets are μm and νn, respectively, we have $\mu m=\nu n$. Hence $\frac{1}{m}\sum_\rho\lambda(m\rho)=\frac{1}{n}\sum_\rho\lambda(n\rho)$. On the other hand we can elementarily prove that $\sum_\rho\lambda(s\rho)=(p-1)\varphi(p-1)/2$ for $s\not\equiv 0$ mod. $p-1$. So we get $m=n$. From this fact, combined with (11) and (12), the equivalence classes of the $\tau_j(\chi^t)$ are represented by $\tau(\chi^m)$, where m runs over all divisors of $p-1$ except $m=p-1$. Now because of the expression (2)′, we easily see that $\tau_j(\chi^t)=\tau_i(\chi^s)$, if and only if $t=s$ and $\operatorname{Ind} j\equiv\operatorname{Ind} i$ mod. $\frac{p-1}{(t,\,p-1)}$, where we put $\operatorname{Ind} j=\nu$, if $j\equiv\omega^\nu$ mod. p, ω being a generator of the group of prime residue classes mod. p. From this and (13)′, we conclude that $\boldsymbol{Q}_{\tau(\chi^t)}=K_{p-1}\cap\boldsymbol{Q}(\tau(\chi^t))$, and we can determine the prime ideal decomposition of $\tau(\chi^t)^{p-1}$ in $\boldsymbol{Q}_{\tau(\chi^t)}$. On account of what has been outlined, Theorem 3 will be obtained.

§3. According to the notation of (3), the Tate group $T_l(J_a)$ is the direct sum of the Tate groups $T_l(A_i)$. The elements α of the automorphism group G induce the endomorphisms $\xi_\alpha^{(i)}$ on each A_i, so that we obtain representations $M_l(\xi_\alpha^{(i)})$ of G ($i=1,\cdots,h$). The l-adic representation $M_l(\xi_\alpha)$ of G on $T_l(J_a)$ is the direct sum of the $M_l(\xi_\alpha^{(i)})$. We shall determine the representation $M_l(\xi_\alpha^{(1)})$ on the main component $A=A_1$.

THEOREM 4. *The representation $M_l(\xi_\alpha^{(1)})$ of G on $T_l(A)$ is the direct sum of the irreducible representations ψ^ν of multiplicity one, where ν runs through the numbers such that $1\leqq\nu\leqq(p^a-1)(p-1)$ and $(\nu,(p^a-1)(p-1))=1$.*

PROOF. As A is a simple abelian variety, $\mathcal{A}_0(A)$ is a division algebra. Hence the characteristic roots of $M_l(\xi_\sigma^{(1)})$ are conjugate to each other, where σ is defined by (1). Now the characteristic roots of $M_l(\xi_\sigma)$ are, by Theorem 1, $\{\psi^\nu(\sigma)\,;1\leqq\nu\leqq(p^a-1)(p-1),\ \nu\not\equiv 0 \text{ mod. } p^a-1\}$. So the number of such characteristic roots that are conjugate to $\psi^\mu(\sigma)$ is equal to $\varphi\left(\frac{(p^a-1)(p-1)}{d}\right)$, $d=(\mu,(p^a-1)(p-1))$. If we assume $d>1$, then we have

$$\varphi\left(\frac{(p^a-1)(p-1)}{d}\right) < \varphi((p^a-1)(p-1)).$$

But the right side is just equal to $2 \dim A=(p-1)\varphi(p^a-1)$. Therefore the characteristic roots of $M_l(\xi_\sigma^{(1)})$ must be $\{\psi^\mu(\sigma)\,;\,1\leqq\mu\leqq(p^a-1)(p-1),\ (\mu,(p^a-1)(p-1))=1\}$, that proves the theorem.

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

Hereafter we write simply $\xi_\sigma^{(1)}=\xi_\sigma$. The endomorphism algebra $\mathcal{A}_0(A)$ of A contains the field $\boldsymbol{Q}(\xi_\sigma)$ of degree $2\dim A=(p-1)\varphi(p^a-1)$ over $\boldsymbol{Q}$. The p-th power endomorphism of J_a induce an endomorphism of A, which is denoted by Π. Since $\Pi\xi_\sigma=\xi_\sigma^p\Pi$, we get $\Pi^{a(p-1)}\xi_\sigma=\xi_\sigma\Pi^{a(p-1)}$ because of Lemma 1. Consequently $\Pi^{a(p-1)}$ is in $\boldsymbol{Q}(\xi_\sigma)$. Let K denote the decomposition field of p in $\boldsymbol{Q}(\xi_\sigma)$. Then, by Lemma 1, K is also the decomposition field of p in K_{p^a-1}. On account of $\Pi\xi_\sigma\Pi^{-1}=\xi_\sigma^p$, the mapping $\eta:\gamma\to\Pi\gamma\Pi^{-1}$ $(\gamma\in\boldsymbol{Q}(\xi_\sigma))$ is a generator of the Galois group of $\boldsymbol{Q}(\xi_\sigma)$ over K. Since $\Pi^{a(p-1)}$ is fixed by η, $\Pi^{a(p-1)}$ is in K. Thus we conclude that the algebra $\boldsymbol{Q}(\Pi,\xi_\sigma)$ which is generated by Π and ξ_σ, is a cyclic algebra over K: $(\Pi^{a(p-1)},\boldsymbol{Q}(\xi_\sigma),\eta)$. The rank of this algebra over K is equal to $[\boldsymbol{Q}(\xi_\sigma):K]^2=a^2(p-1)^2$. By the way, Proposition 2 shows that the field K is the center of $\mathcal{A}_0(A)$. Since $\mathcal{A}_0(A)$ contains the field $\boldsymbol{Q}(\xi_\sigma)$ of degree $2\dim A$, its rank over the center K must be $[\boldsymbol{Q}(\xi_\sigma):K]^2$. Thus we have proved the following

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

$$(\Pi^{a(p-1)},\boldsymbol{Q}(\xi_\sigma),\eta)$$

where σ is the automorphism of the curve C_a defined by (1), and η is a generating automorphism of $\boldsymbol{Q}(\xi_\sigma)$ over K.

Tokyo Metropolitan University

References

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

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

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

[4] T. Yamada, On the jacobian varieties of Davenport-Hasse curves, Proc. Japan Acad., 43 (1967), 407-411.