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

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

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

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

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

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

The previous automorphism σ is given in this case by

$$(2)'\qquad \sigma\colon (z, x)\to(z, \theta x).$$

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